2X Product Manual

ApplicationServer XG Version 11

Last updated: 2013-10-09

Table of Contents

Introduction to 2X ApplicationServer 1
What is 2X ApplicationServer? 1
How does it work? 1
About This Document 1
Introduction 1
Terminology 2
What is new in Version 11 2
Multiple Remote Sites 2
Multiple Administrators and Roles 3
Collaboration 3
Improved Manageability 3
Improved Accountability 3
Easy Backup and Restore of 2X Farm Configuration 3
Improved Publishing 3
Improved Published Resources Filtering Options 3
Improved Client Management 3
Improved 2X OS 4
Other Major Improvements in 2X ApplicationServer XG 11 4
Licensing 2X ApplicationServer XG 4
Installing 2X ApplicationServer 5
System Requirements 5
Installing 2X ApplicationServer 5
Configuring a 2X ApplicationServer XG Administrator Account 6
2X ApplicationServer XG Getting Started 7
Introduction 7
2X ApplicationServer Console 7
Introduction 7
2X ApplicationServer Console Layout 7
Setting Up an SMB Environment 8
Add a Terminal Server 8
Publish an Application 9
Publish a Desktop 10
Sites & Administrators 12
Introduction 12
Sites 12
Introduction 12

Adding a New Site to the Farm 13
Accessing Site Configuration 15
Switching Between Sites Configurations 15
Managing Sites 16
Replicating Site Settings to all Sites 16
Setting a Site as a Licensing Server 17
Administrators 18
Introduction 18
Default 2X ApplicationServer XG Administrator 18
Adding an Administrator Account 18
Configuring Administrator Accounts Permissions 19
Managing Administrator Accounts 20
Sending Console Messages between Administrator Accounts 20
Logging off Other Administrators 21
Terminal Servers 22
Introduction 22
Adding a Terminal Server 22
Installing the 2X Terminal Server Agent Manually 23
2X Terminal Server Agent System Requirements 23
Installing the 2X Terminal Server Agent Manually 23
Configuring a Terminal Server 24
Enabling or Disabling a Terminal Servers 24
Configuring Server Name and Maximum Sessions 25
Configuring the 2X Terminal Server Agent on the Server 25
Configuring RDP Printing for Terminal Server 27
Configuring Terminal Server Maintenance Time Window 27
Grouping Terminal Servers 29
Publishing a Desktop from a Terminal Server 29
Publishing an Application from a Terminal Server 31
Configuring a Single Application 32
Publishing a Document from a Terminal Server 33
VDI Hosts 36
Introduction 36
Adding a VDI Host 36
Installing the 2X VDI Agent Manually 37
2X VDI Agent System Requirements 37
Installing the 2X VDI Agent Manually 37
Installing an Appliance 38

Introduction 38
Installing the Appliance 38
Configuring a VDI Host 38
Enabling or Disabling a VDI Servers in the Farm 39
Configuring VDI Host Connection Settings 39
Configuring the 2X VDI Agent on the Server 39
Configuring RDP Printing for VDI Host 40
Configuring VDI Host Maintenance Time Window 41
Configuring and Managing Pools 42
Introduction 42
Adding and Deleting Pools 42
Managing Members in a Pool 43
Configuring and Managing 2X Templates for Guest Clones 44
Introduction 44
Creating a 2X Template 45
Configuring a 2X Template 46
Configuring SysPrep for Virtual Guest Clones 48
Updating the Template Operating System 49
Persistent Guests 49
Deleting a Persistent Guest Rule 50
Configuring Automatic Deleting of Persistent Guest Rules 50
Publishing a Virtual Desktop from a Guest 50
Publishing an Application from a Guest 52
Publishing a Document from a Guest 53
Remote PCs 56
Introduction 56
Adding a Remote PC 56
Installing the 2X Remote PC Agent Manually 58
2X Remote PC Agent System Requirements 58
Installing the 2X Remote PC Agent Manually 58
Configuring a Remote PC 59
Enabling or Disabling a Remote PC in the Farm 59
Configuring or Changing a Remote PC IP Address 59
Configuring the Remote PC Agent 60
Configuring RDP Printing for Remote PC 61
Publishing a Desktop from a Remote PC 62
Publishing an Application from a Remote PC 62
Publishing a Document from a Remote PC 64

Publishing and Filtering 66
Introduction 66
Managing Published Applications 66
Publishing an Application 66
Configuring a Published Application 66
Managing Published Desktops 74
Publishing a Desktop 74
Configuring a Published Desktop 74
Managing Published Documents 79
Publishing a Document 79
Configuring a Published Document 79
Managing Published Folders 84
Introduction 84
Publishing a Folder 84
Managing Published Folders 85
Adding Published Resources to a Folder 85
Filtering 86
Introduction 86
Creating New Filtering Rules 86
Filtering by User 86
Filtering by Client 87
Filtering by IP Address 89
Filtering by MAC Address 90
Filtering by Gateway 92
Configuring Multiple Filtering Rules 92
2X Secure Client Gateways 93
Introduction 93
How a Gateway Works 93
2X Secure Client Gateway Types 94
Normal Mode 94
Forward Mode 94
Adding a 2X Secure Client Gateway 94
Manually Adding a 2X Secure Client Gateway 96
Managing 2X Secure Client Gateways 98
Introduction 98
Enabling and Disabling a Gateway 98
Configuring the 2X Secure Client Gateway Port 99
Configuring Thin Client and 2XOS Support 100

Enabling SSL Encryption on 2X Secure Client Gateway 101
Enabling HTML 5 Support on the Gateway 103
Configuring HTML 5 Connection User Capabilities 103
Accessing the HTML 5 Interface 104
Changing the Gateway Mode and Forwarding Settings 104
Managing Multiple IP Addresses on a Gateway 105
Support for Wyse Thin Client OS 105
Filtering Access to 2X Secure Client Gateway 106
Miscellaneous Gateway Settings 106
Gateway Tunnelling Policies 107
Introduction 107
Configuring Tunnelling Policies 107
2X Backup Servers 109
Introduction 109
Adding a 2X Backup Server 109
Managing Backup Servers 110
Enabling or Disabling Backup Servers 110
Changing Backup Servers Priority 110
Promoting a Backup Server to Master Server 111
Deleting Backup Servers 111
Load Balancing 112
Introduction 112
Resource Based Load Balancing 113
Enabling Resource Based Load Balancing 113
Configuring Resource Counters 113
Round Robin Load Balancing 114
Enabling Round Robin Load Balancing 114
Advanced Load Balancing Settings 114
Session Management 114
Configure Servers Connection and Uptime Test 114
Excluding a Process from the CPU Counter 114
2X Universal Printing 116
Introduction 116
Managing 2X Universal Printing Servers 116
Enabling and Disabling the 2X Universal Printing Support 117
Configuring a Printer Renaming Pattern 117
Fonts Management 117
Excluding Fonts from Embedding 118

Automatically Install Fonts on Servers and Clients 118
Resetting List of Excluded Fonts to Default 118
2X Universal Scanning 119
Introduction 119
Managing 2X Universal Scanning 120
Enabling and Disabling 2X Universal Scanning Support 120
Managing Scanning Applications 120
Adding a Scanning Application 120
Deleting a Scanning Application 121
Installing 2XOS and Network Booting 122
Introduction 122
Network Booting a Device Running 2XOS 122
1. Configure Thin Client Support on Gateway 122
2. Choose and Install the Required 2X Operating System(s) 122
3. Configure the Device and Boot It 123
Installing 2XOS on Thin Client or PC Permanent Storage 123
Unattended Install of 2XOS on Thin Client or PC Permanent Storage 126
Creating a Bootable USB Stick That Matches Your Device 126
Managing Devices and Thin Clients 127
Introduction 127
Monitoring Devices 127
Introduction 127
Device Statuses 127
2XOS 128
Introduction 128
Making a Version of 2XOS Available for Thin Clients 128
Configuring a Version of the 2XOS as Default 129
Adding a Thin Client 129
Thin Clients Groups 131
Introduction 131
Creating a Thin Clients Group 131
Configuring Thin Client Options in Groups 132
Configuring Hardware Options, OS, Booting Options and Method 132
Configuring Auto Login Options 133
Configuring Regional Settings 133
Configuring Input Devices 133
Configuring Screen Saver 134
Configuring Desktop 134

Configuring Browser 134
Configuring Remote Desktop Options 134
Configuring Thin Client in Kiosk Mode 134
Configuring List of Locally Installed Applications 134
Configuring Shadowing 135
Configuring RDP Default settings 135
Configuring Thin Client Options 136
Configuring Thin Client Printers 136
Adding a Printer to the List 136
Assigning a Printer or Multiple Printers to a Thin Client or Group 137
Configuring a Custom 2XOS Log In Banner 137
Scheduling Thin Clients Auto Power On, Off or Restart 137
Introduction 137
Adding a New Schedule 137
Managing Schedules 138
Managing 2X Client Settings 139
Introduction 139
Adding a New 2X Client Policy 139
Reporting 141
Introduction 141
Integrating with eG Innovations Reporting Engine 141
Configuring the Connection 141
Configuring the Reporting Agents 142
More Information 144
Connection & Authentication Settings 145
2X Publishing Agent Connection Settings 145
Enforcing Authentication 145
Configuring Authenticating 145
Authenticating Against Non Domain Users 146
Second Level Authentication 146
How it Works 146
Configuring Deepnet Authentication Server 146
Configuring Safenet Server 146
Configuring Radius Server 146
Restricting Access by OS Build Number 146
Managing the 2X ApplicationServer XG 148
Introduction 148
2X ApplicationServer XG Status 148

Configuring Monitoring Counters and Email Alerts 149
Configuring Monitoring Counters 149
Configuring SMTP Server Connection for System Notifications via Email 149
Configuring Notification Intervals 150
Monitoring 2X ApplicationServer XG Configuration Changes 150
Configuration Changes Notifications in 2X ApplicationServer XG Console 152
Configuring Logging 153
2X ApplicationServer XG Auditing Logging 153
2X ApplicationServer XG Logging Per Server 154
2X ApplicationServer XG Logging Per Site 155
Keeping 2X ApplicationServer XG Up to Date 156
Backing up the 2X ApplicationServer XG Configuration 156
Appendix 157
2XOS Supported Features 157
TROUBLESHOOTING AND SUPPORT 158
Introduction 158
Knowledgebase 158
Request Support via E-mail 158
Request Support via Phone 158
ABOUT 2X 159

Introduction to 2X ApplicationServer

What is 2X ApplicationServer?

2X ApplicationServer XG provides vendor independent virtual desktop and application delivery from a single platform. Accessible from anywhere with native clients and web enabled solutions like the 2X Cloud Portal, 2X ApplicationServer XG allows you to publish full desktops, applications and documents within a virtual environment, improving desktop manageability, security and performance.

2X ApplicationServer XG extends Windows Terminal Services by using a customized shell and virtual channel extensions over the Microsoft RDP protocol. It supports all major Hypervisors from Microsoft, VMware, Citrix and more enabling the publishing of virtual desktops and applications to the 2X Client.

The product includes powerful universal printing and scanning functionality, high capacity resource based load balancing and management features.

With the 2X ClientManager Module for 2X ApplicationServer XG you can also centrally manage user connections, thin client and PCs converted into thin clients using the free 2XOS.

How does it work?

When a user requests a virtual desktop or application, the system finds a guest on one of the least loaded hosts and starts or restores the guest connection. Using Microsoft RDP protocol, the virtual desktop or publish application is presented to the user.

Users can connect to the 2X ApplicationServer XG using a thin client running the free 2XOS or by using the 2X Client which can run on Windows, Linux, MAC, Android, Blackberry, Chrome and iOS. Users can also connect via an HTML 5 browser.

Thin client computing is solving the growing management problem of fat clients (PC's), allowing employees to roam easily and seamlessly, improving performance. Companies that have migrated to a thin client environment consistently see huge savings on support, hardware and upgrade costs. In a world where energy use is an increasing concern, implementing a thin client environment improves energy costs as well. A study conducted by Bloor Research shows that "Deploying thin client technology across enterprises can cut costs by up to 70%".

About This Document

Introduction

This product manual assumes that the reader is familiar with Microsoft Terminal Server and has an intermediate networking knowledge.

All Titles, labels and names (such as product features, buttons and links) will be displayed in **bold**.

Terminology

Category
A category consists of a number of settings related to a specific task or operation. In the 2X ApplicationServer Console the following categories are available:

- Farm
- Load Balancing
- Publishing
- Universal Printing
- Universal Scanning
- Connection
- Client Manager
- Administration
- Information
- Reporting
- Licensing

Farm
A farm consists of a 2X ApplicationServer XG installation on a site or multiple sites.

Licensing Server Site
The site where the main configuration database is stored and manages all other sites in the 2X Farm. Other servers in a site can be upgraded to Licensing Server if the main licensing server is not available. **Note:** Upgrades of the 2X ApplicationServer XG MUST be applied to the licensing server site first.

Publishing
The act of making items installed on a Remote Desktop Server, VDI Host or Remote PC available to the users via the 2X ApplicationServer XG.

Publishing Agent
The Publishing Agent provides load balancing of published applications and desktops.

RDS
Remote Desktop Services is a server role in Windows Server that provides technologies to enable users to connect to virtual desktops and session-based desktops. RDS replaced Terminal Services beginning in Windows 2008 R2.

Site
A site consists of a publishing agent, a SecureClient GW or multiple gateways and the agents installed on the Terminal Servers, VDIs and PCs.

What is new in Version 11

The new 2X ApplicationServer XG version 11 focuses on scalability and collaboration. Highlights of the new features are:

Multiple Remote Sites

Ideal for companies with remote locations and overseas offices, multiple sites can be installed in a single 2X ApplicationServer XG farm and managed from a central location. A single site is what previously was a farm and upon installation, a 2X farm will have a single site. Each site can have multiple gateways (and publishing agents) through which users can connect to access published resources.

Sites can be managed from the new **Farm** category in the 2X ApplicationServer Console.

Multiple Administrators and Roles

Multiple administrators from the company's network can be configured as 2X farm administrators. Granular permissions for each administrator can be configured, for example an administrator can only change the configuration of a specific site or function, such as universal printing.

Administrators and their permissions can be managed from the new **Administration** category in the 2X ApplicationServer Console.

Collaboration

When multiple administrators are logged on to the 2X ApplicationServer Console they can communicate with each other by sending messages via the console. Any changes done by other administrators is notified to the logged on administrator in real time.

Logged on administrators with full permissions can also remotely log off other administrators via the Administrators dialog box.

Improved Manageability

From the 2X ApplicationServer Console an administrator can switch from a site's configuration to another by selecting the site from a drop down menu in the new **Site and Logged On User** bar at the top of the 2X ApplicationServer Console (if the administrator has the permission to access the configuration of the selected site).

Any configuration changes applied to a specific site, such as Universal Printing options, Universal Scanning Options, Publishing of resources etc can be replicated to all sites on the farm at the click of a button.

Improved Accountability

All of the administrators' activity is logged for accountability in the **Settings Audit** tab in the **Administration** category. The last applied changed by any logged on administrator also shows up in the new **Notification Bar** available at the bottom left of the 2X ApplicationServer Console.

Easy Backup and Restore of 2X Farm Configuration

The 2X ApplicationServer XG Farm configuration can now be easily backed up and restored by using the Import and Export functions in the **Backup** tab from the **Administration** category in the 2X ApplicationServer Console.

Improved Publishing

When a resource is published, it can be published to all the sites or to a specific or specific number of sites. Published resource name, description, icon and run as settings are shared through all the sites.

Improved Published Resources Filtering Options

Version 11 supports filtering rules based on the gateway. For example you can filter a connection based on the gateway through which the connection is being established.

Improved Client Management

The hardware manufacturer and model of thin clients can now be preconfigured. This means that administrators no longer have to configure boot parameters and other type of settings related to the thin client hardware.

Improved 2X OS

The new 2X OS boots faster and has a faster runtime. It also has the following improvements:

- SMB file access support
- Supports WINS name resolution
- USB drives are mounted on the fly
- Safe eject of USB devices
- Network time protocol settings
- Welcome screen shows the OS version
- Cursor Theme, Menus and Icons have been upgraded

Other Major Improvements in 2X ApplicationServer XG 11

- Terminal Servers and Terminal Servers Groups configuration has been split in 2 tabs
- Tunnelled Policies have been moved to the Gateway node
- 2X Agents logging options can be configured from a single tab
- Do Not Redirect URL list option under Site Settings is global for all servers in the site
- HTML 5 connection support can now be configured from the 2X Gateway properties
- Tunnelling Policies lists are now available in the Gateways node
- Advanced settings of published resources are available in their own tab
- New PDF converter that improves the quality and reduces the site of print jobs
- Faster universal scanning protocol
- Published Item Listings has been renamed to Access Devices. From this tab the administrator can also control the runtime sessions
- Multiple printers can now be configured for clients running 2X OS
- Support for network and USB printers for clients running 2X OS
- Local applications support for 2X OS (Skype, Adobe Reader, Media Player, Calculator and more can be included in the client groups)

Licensing 2X ApplicationServer XG

2X ApplicationServer XG is licensed based on the number of concurrent users. A new base license pack consists of a minimum of 15 users.

New license purchases include one year of Upgrade Insurance and a Bronze Support Package for 7 days. Upgrade Insurance entitles customers to receive the latest product version upgrades for a 12-month period from the date of license activation. Should customers want to take up the product for more than 1 year, license packs for 2 and 3 years are readily available.

For more information about the 2X ApplicationServer XG licensing refer to the following URL: http://www.2x.com/applicationserver/licensing/

Installing 2X ApplicationServer

System Requirements

The 2X ApplicationServer XG core components (2X Publishing Agent and 2X SecureClientGateway) should be installed on Windows 2003, Windows 2008, Windows 2008 R2 and Windows 2012 Server operating system.

Recommendation: The 2X ApplicationServer XG should not be installed on a domain controller or any other server where a DHCP server is running.

2X Terminal Server Agents should be installed on Windows 2003 SP1, Windows 2008, Windows 2008 R2 and Windows 2012 Server operating system with Terminal Services enabled.

2X Client is approved for the following operating systems:

- Windows XP SP3
- Windows Vista
- Windows 2003 SP1
- Windows 7
- Windows 8. 8.1
- Windows CE
- Windows Embedded
- Mac 10.5.x and above
- iOS (iPhone and iPad)
- Android 1.5 and above
- Ubuntu 8.04, 8.10, 9.04, 9.10
- OpenSuse 11.1
- Fedora Core 9, 11
- CentOs 5.2
- VectorLinux 6.0

Installing 2X ApplicationServer

Note: You should be logged in with an account that has administrative privileges to install 2X ApplicationServer XG. Close all other Windows programs before running the installation.

1. Login to the machine and download the latest version of the 2X Application Server from the 2X website.
2. Double click the 2xAppServer.msi to launch the 2X ApplicationServer XG installation wizard. Click **Next** when prompted.
3. Review and approve the end-user license agreement and click **Next**.
4. Specify the folder location where 2X ApplicationServer XG will be installed and click **Next**.

5. Select the option **2X ApplicationServer XG** for a default installation of the 2X ApplicationServer XG and click **Next**.
6. Click **Install** to start the installation. The setup will now copy all files and install the 2X Application Server services.
7. Click **Finish** when ready.

Configuring a 2X ApplicationServer XG Administrator Account

The first time you launch the 2X ApplicationServer XG Console you have to specify a username and password, as seen in the below screenshot. The user specified will be automatically configured as the 2X ApplicationServer XG administrator. Use any user from the active directory or machine to login where the 2X ApplicationServer XG is installed.

2X ApplicationServer XG Console First Time Login Prompt

For more information about 2X ApplicationServer XG administrators and privileges refer to the chapter Administrators on page 18.

2X ApplicationServer XG Getting Started

Introduction

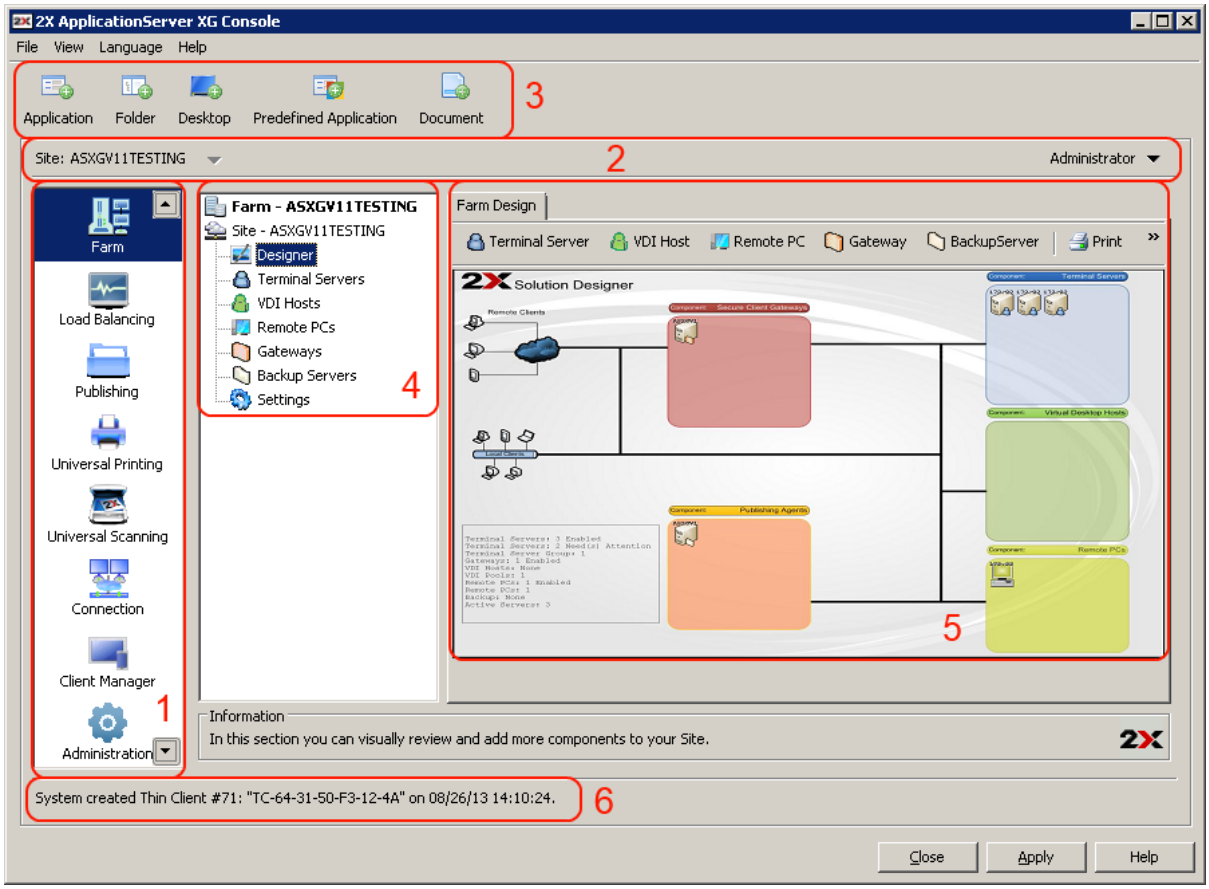
One of the fundamental features of 2X ApplicationServer XG is the ability to publish seamless applications individually to your users. This means users will only see the applications you give them access to and not a full terminal service desktop

2X ApplicationServer Console

Introduction

The 2X ApplicationServer Console is from where you can manage 2X ApplicationServer XG. Use the console to publish an application or desktop, add a terminal server of VDI host to the farm, backup the 2X ApplicationServer XG configuration and all other configuration changes.

2X ApplicationServer Console Layout



2X ApplicationServer Console

Section 1: This section contains all the categories.

Section 2: This information bar displays the site you are currently logged in on the left and the user currently logged in on the right.

Section 3: Toolbar from where you can launch the publishing wizards.

Section 4: Available only in the Farm and Publishing category, the navigation tree allows you to browse through the objects related to that category.

Section 5: This section displays the selected object or category properties, such as servers in a farm or published application properties.

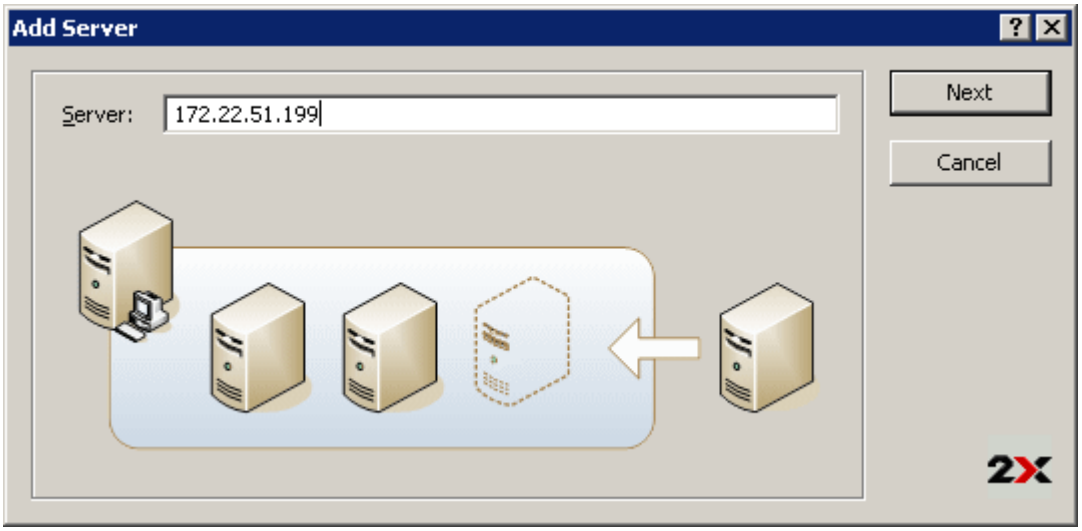
Section 6: In this section the latest console notification are displayed.

Setting Up an SMB Environment

This getting started guide explains how to add the server where the 2X ApplicationServer XG is installed as terminal server to a site in the farm and publish an application (2X Application Server Console) from it.

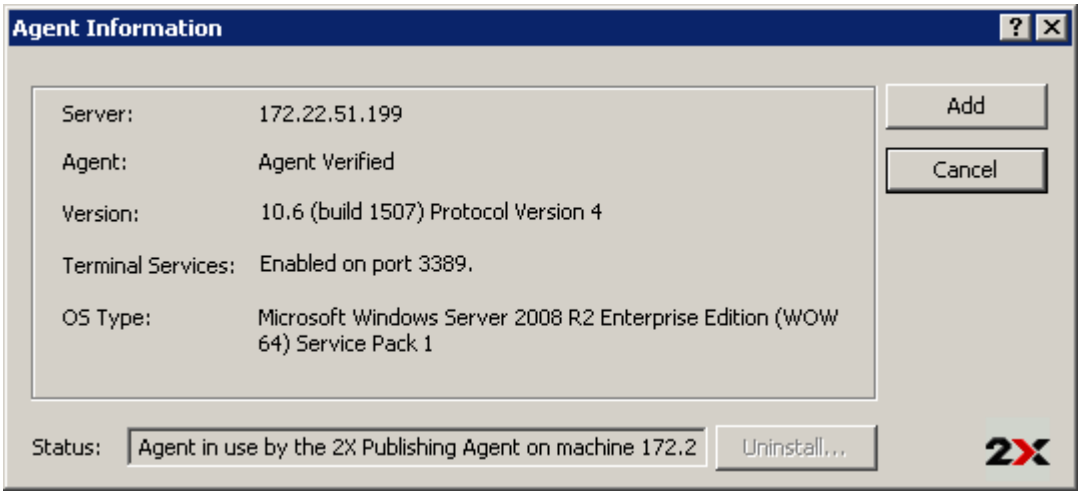
Add a Terminal Server

1. Launch the 2X ApplicationServer Console, select the **Farm** category and click on **Terminal Servers** from the navigation tree.
2. Select **Add** from the **Tasks** drop down menu to launch the setup wizard and once prompted enter the server FQDN or IP. In this case enter the IP address of the 2X ApplicationServer XG server and click **Next**.



First Step of the Terminal Server Wizard

3. In the next step the 2X ApplicationServer XG checks if the 2X Agent is installed on the server. Once confirmed click **Add** to add the server to the farm.

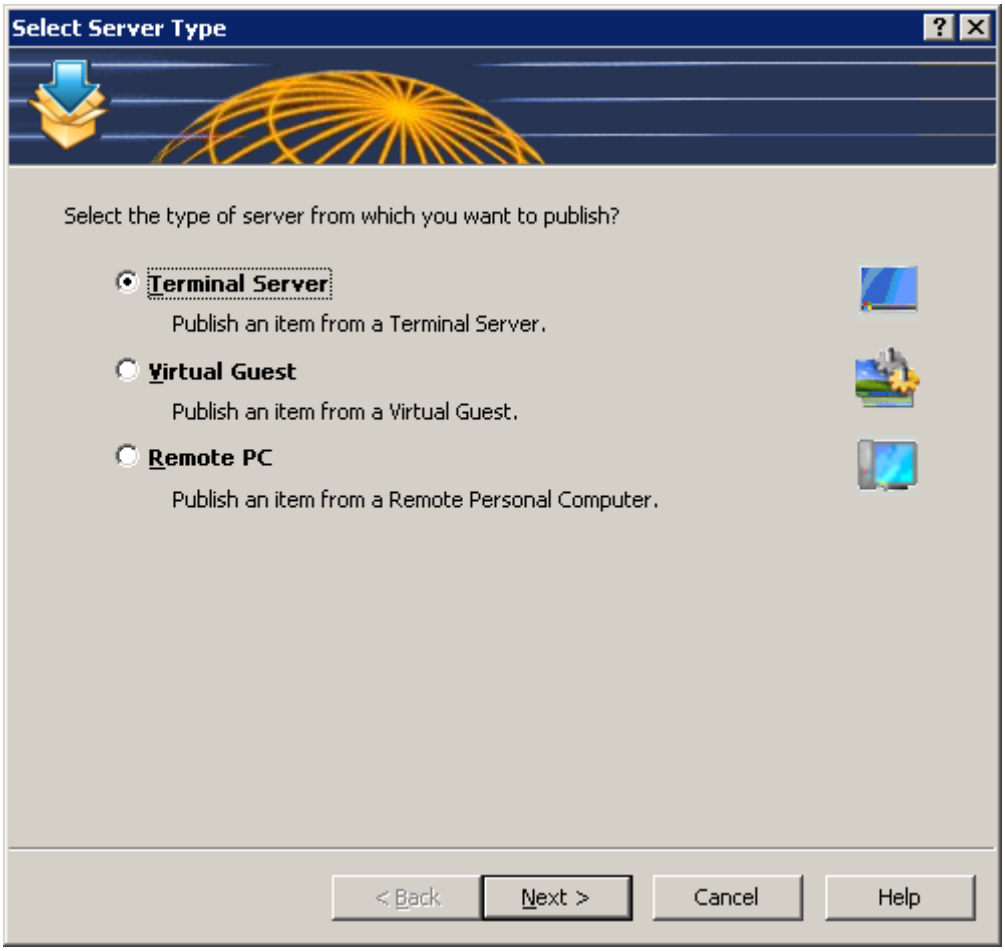


2X Terminal Server Agent Check

Publish an Application

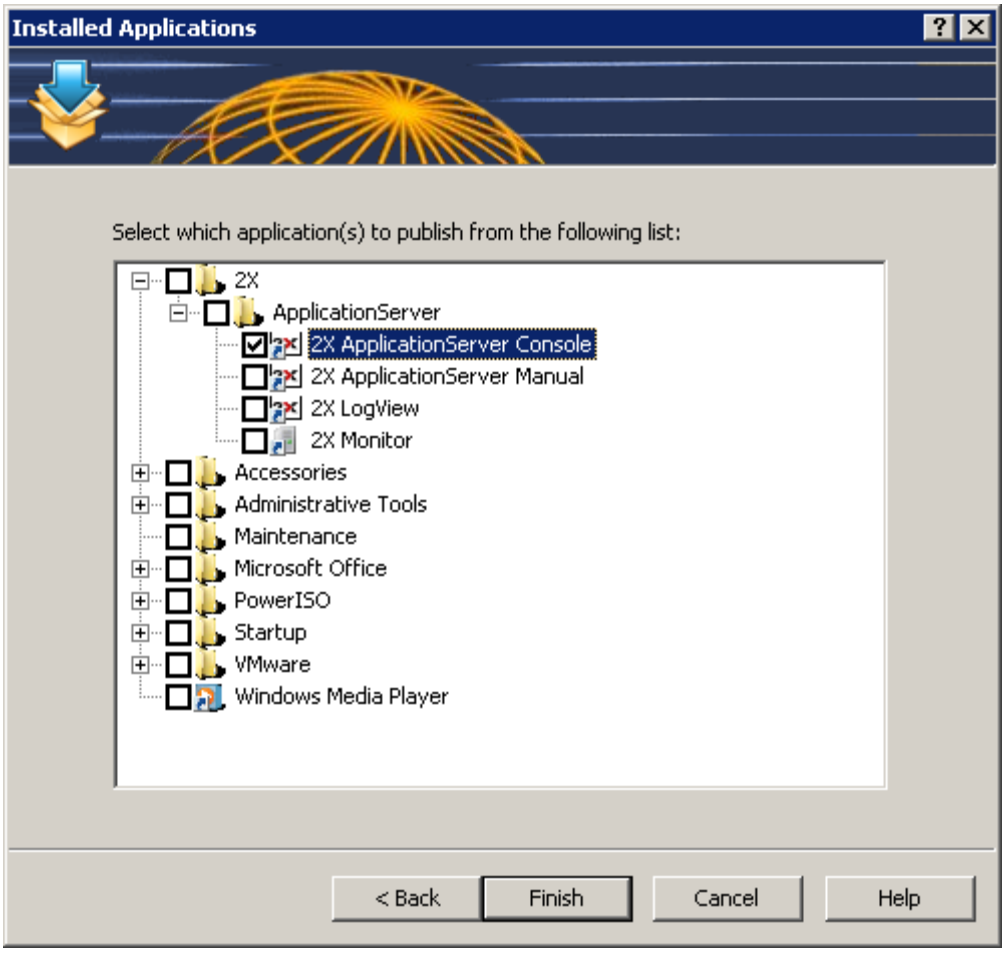
The below procedure explains how to publish the 2X ApplicationServer XG Console as an application, but you can publish any other application you like.

1. Click the **Publishing** category and click the **Application** icon from the console top menu to launch the wizard.


Select Server Type
Select the type of server from which you want to publish?
Terminal Server
Publish an item from a Terminal Server.
Virtual Guest
Publish an item from a Virtual Guest.
Remote PC
Publish an item from a Remote Personal Computer.
< Back
Next >
Cancel
Help

First Step of the Application Publishing Wizard

2. In the first step of the wizard select **Terminal Server** and click **Next** as seen in the screenshot above.
3. In the second step select **Installed Application** to select the application from a list of installed applications on the server and click **Next**.
4. Expand the **2X** > **Application Server** node and tick **2X ApplicationServer Console** to publish the 2X ApplicationServer console as seen in the screenshot below.



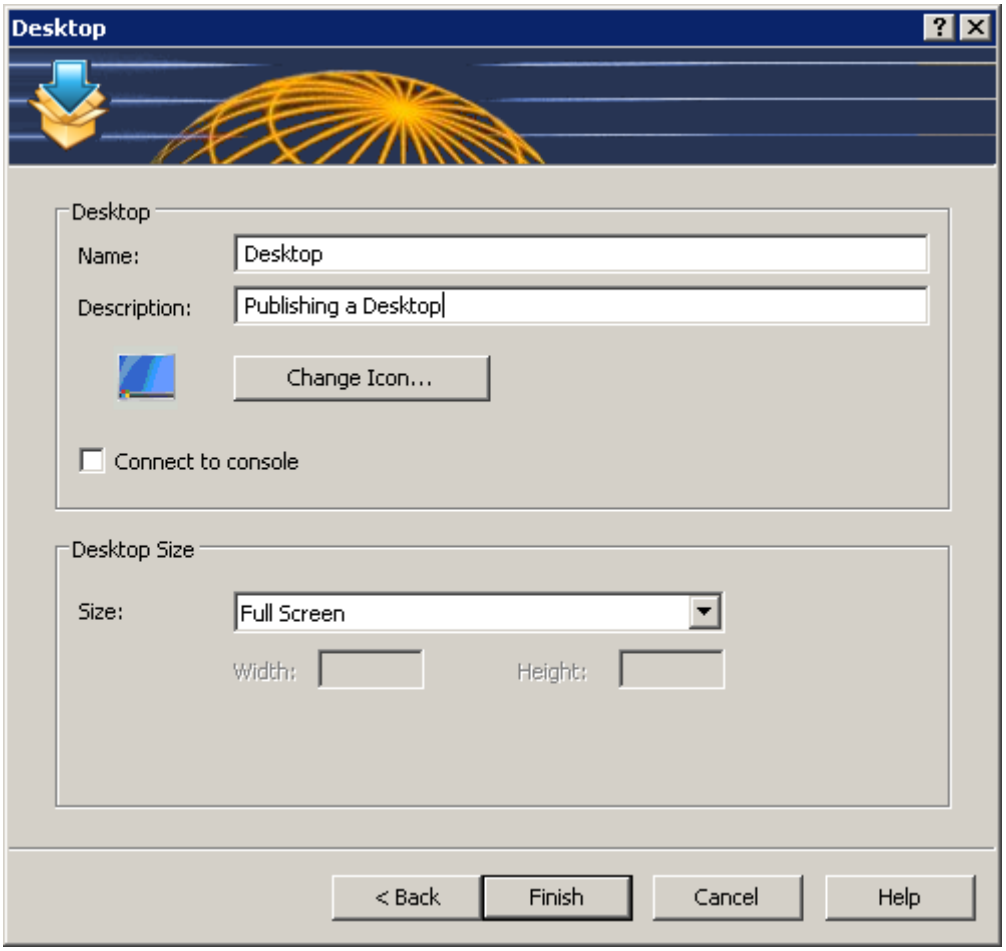
Highlighting the 2X ApplicationServer Console to publish it

5. Click **Finish** when ready.

Publish a Desktop

The below procedure explains how to publish the desktop of the server where the 2X ApplicationServer XG is installed.

1. Click **Publishing** from the system menu and click the **Desktop** icon from the console top menu to launch the wizard.
2. In the first step of the wizard select **Terminal Server Desktop** and click **Next**.
3. In the second step of the wizard you have to specify a **Name** and **Description** for the shared desktop and (optional) change the **Icon**. Enable the option **Connect to console** so users connect to console rather than a virtual session.



Second Step of the Desktop Publishing Wizard

4. As seen from the above screenshot, in the second step of the wizard you can also configure the size and resolution of the desktop from the **Size** drop down menu. Once configured, click **Finish** to publish the desktop.

Sites & Administrators

Introduction

A 2X ApplicationServer XG farm can contain multiple sites which can be administered by different administrators.

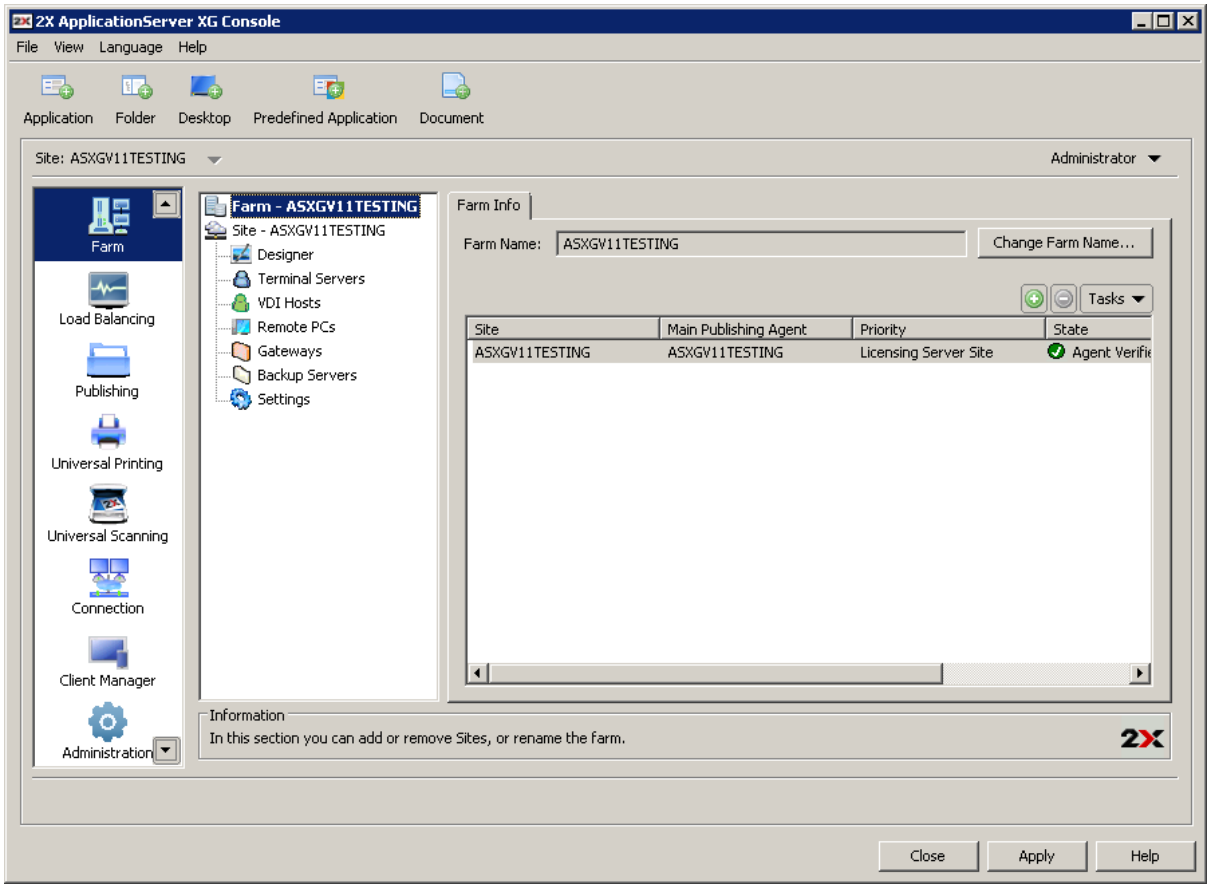
Sites

Introduction

A 2X ApplicationServer XG farm can have multiple sites. Each site consists of a publishing agent, a SecureClient GW or multiple gateways, and the agents installed on the Terminal Servers, VDIs and PCs. At least one server has to be dedicated for a site where the master publishing agent and gateway will be installed.

The first default site added to the 2X ApplicationServer XG farm is the **Licensing Server**, where the main 2X AppliationServer XG configuration database is stored. Every other additional site on the farm will have a synched copy of the configuration database and once changes are applied to a particular site, the Licensing Server database is updated.

Sites can be managed from the **Farm** node in the navigation tree available in the **Farm** category.



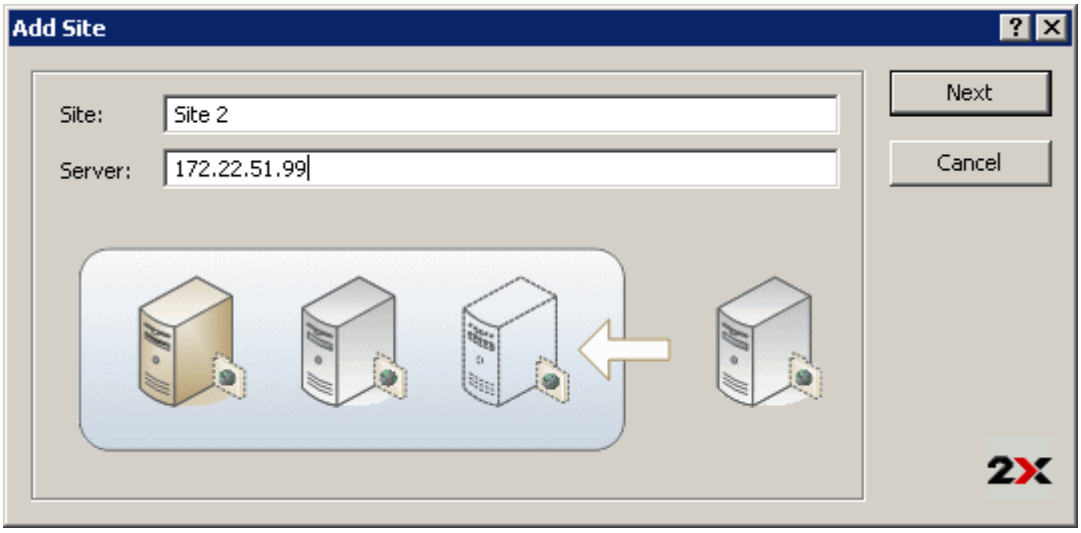
Configuring Sites in 2X ApplicationServer XG

Note: The **Farm** node is only available to administrators which have full permissions on the farm. For more information about administrators and permissions refer to the Administrators section on page 18.

Adding a New Site to the Farm

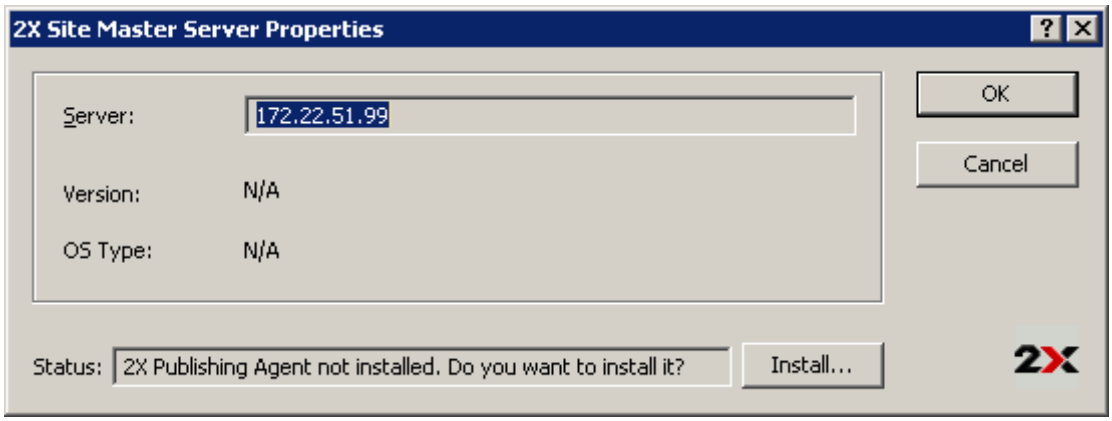
To add a site to the 2X ApplicationServer XG farm follow the below procedure:

1. Click the **Farm** node in the navigation tree and click the **Green Plus** button to launch the Add Site wizard. Alternatively you can also select the **Add** option from the **Tasks** drop down menu.
2. In the first step of the wizard, specify a site name in the **Site** input filed and specify the server IP or FQDN where the master publishing agent and gateway will be installed in the **Server** input field.



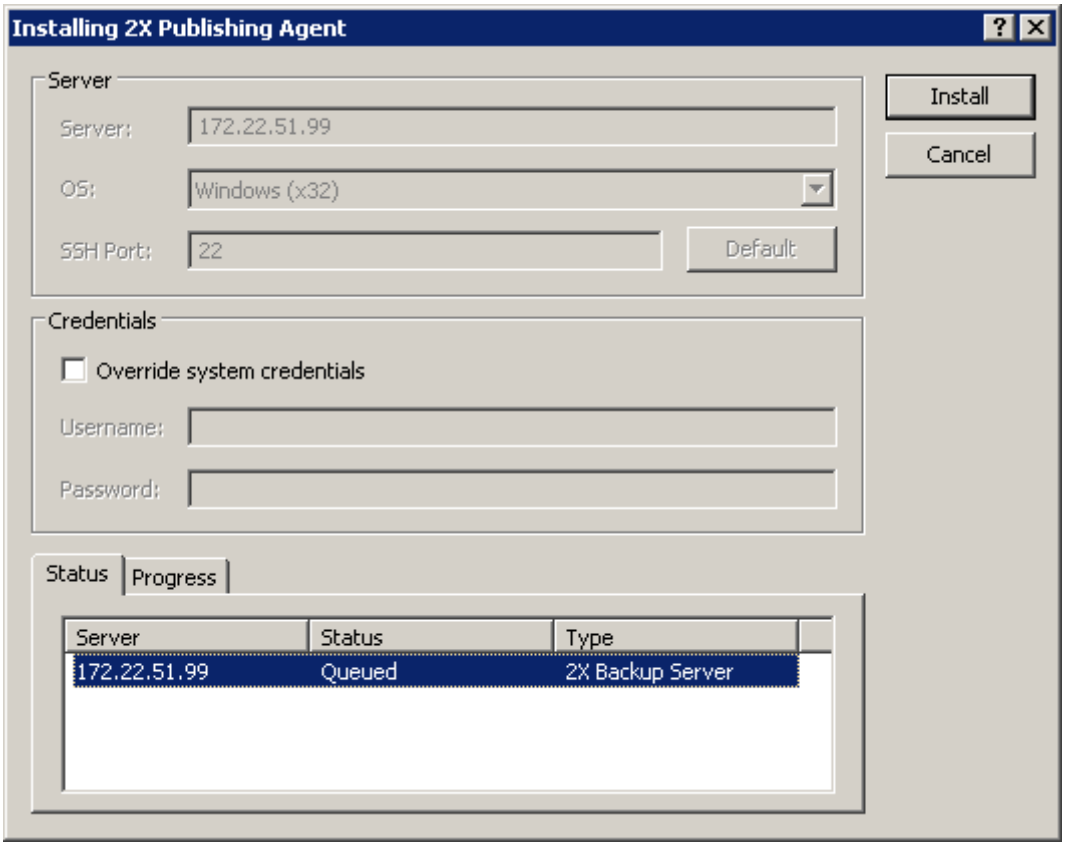
First Step of the Add a New Site Wizard

3. In the second step of the wizard the 2X ApplicationServer XG checks if the 2X Publishing Agent is installed on the site server. If not, click **Install** to proceed with the remote installation.



Second Step of the Add a New Site Wizard – Check for Publishing Agent

4. In the **Installing 2X Publishing Agent** dialog, highlight the server name on which the 2X Publishing Agent is to be installed as seen in the below screenshot.
5. (Optional) Tick the option “Override system credentials” to specify and use different credentials to connect to the server and install the 2X Agent.



Installing 2X Publishing Agent Dialog Box

6. Click **Install** to install the publishing agent and gateway, and click **Done** once it has been successfully installed.
7. In the last step of the Add Site wizard, click **OK**.

Accessing Site Configuration

Once a new site is created you can access its configuration by running the 2X ApplicationServer XG Console on the site server or by switching to its configuration from the 2X ApplicationServer XG Console as explained in the following section **Switching Between Sites Configurations**.

Note: When running the 2X ApplicationServer XG Console you will always be connected to the licensing server database, even if running it from a site server. Once changes are applied, configuration changes are replicated from the licensing server to the site servers.

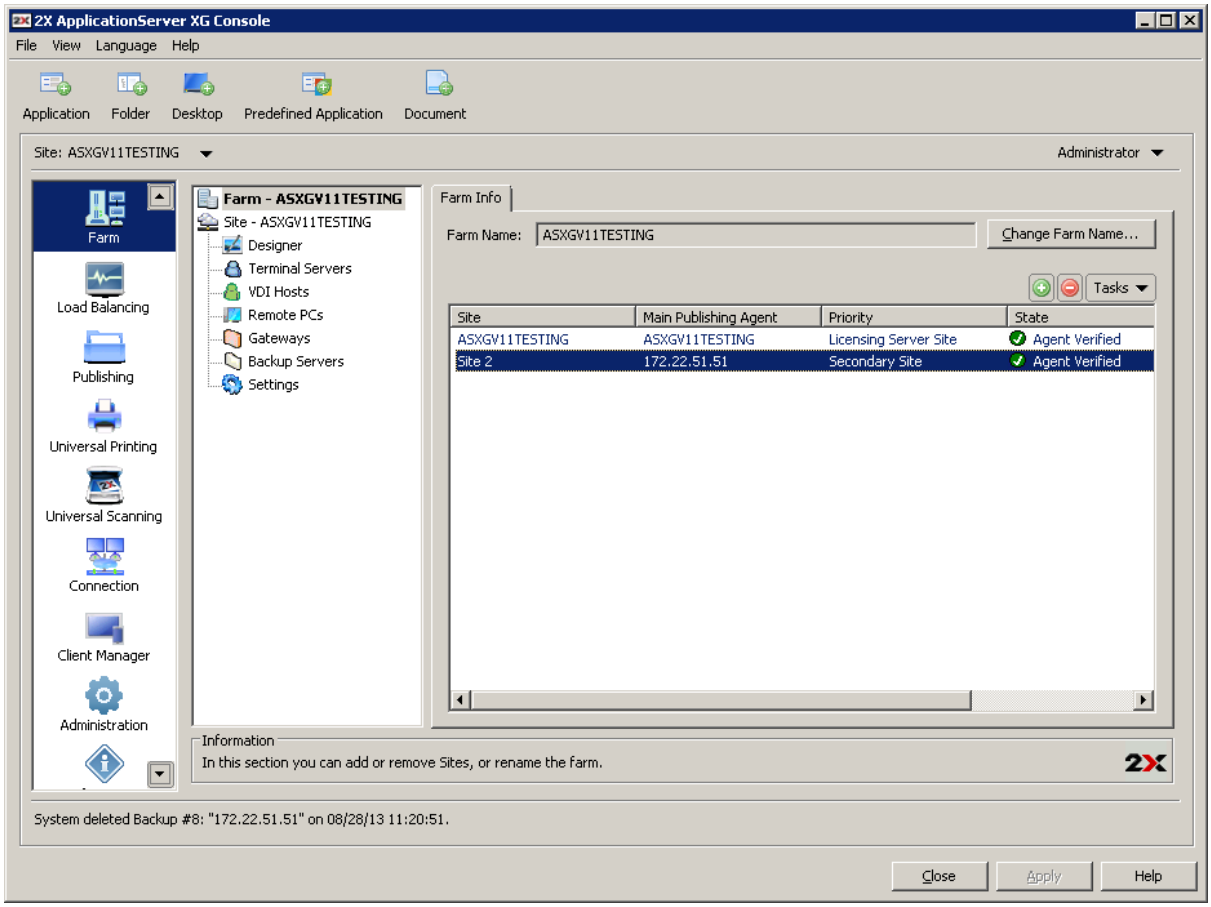
Switching Between Sites Configurations

From the 2X ApplicationServer XG Console you can only view the configuration of one site at a time. If you login as a farm administrator, the configuration of the Licensing Server site will be loaded. If you login with an administrator that has access to a specific site, the configuration of that site will be loaded.

To switch between the configuration of different sites from the 2X ApplicationServer XG Console follow the below procedure:

1. Open the **Farm** category and click on the **Farm** node from the navigation tree to access the list of sites in the farm.

2. Highlight the site you would like to configure and from the **Tasks** drop down menu select **Switch to this Site**. Alternatively you can use the top bar and select the site you want to switch to from the **Site** drop down menu.



Managing Multiple Sites from the Farm Node

Managing Sites

Sites can be managed from the **Farm** node in the navigation tree available in the **Farm** category. From this section you can change the farm name and also add or delete sites.

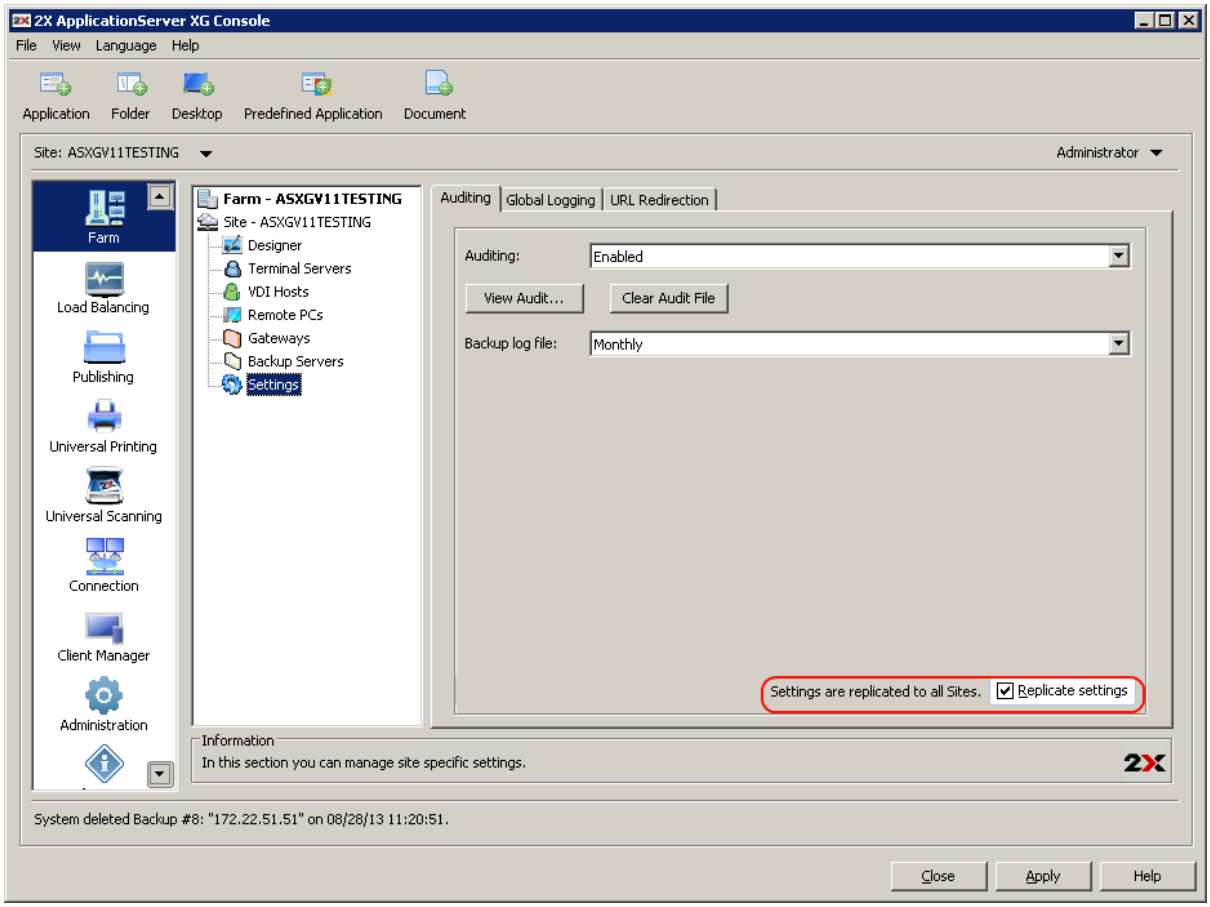
Replicating Site Settings to all Sites

Any setting which is site dependant can be replicated to all other sites. Refer to the below table for more specific information about which settings can be replicated to other sites.

Category	Section	Options
Farm	VDI Hosts, Persistent Guests	Auto removal timeout
Farm	Settings, Auditing	All Settings
Farm	Settings, Global Logging	Logging Settings
Farm	URL Redirection	All Settings
Load Balancing	Load Balancing	All Settings
Publishing	Advanced, Shortcuts	All Settings
Publishing	Advanced, Extensions	All Settings
Publishing	Advanced, Licensing	All Settings
Publishing	Advanced, Display	All Settings
Publishing	Filtering, User	All Settings
Publishing	Filtering, Client	All Settings
Publishing	Filtering, IP Address	All Settings
Publishing	Filtering, MAC	All Settings

Universal Printing	Universal Printing	Printer Renaming
Universal Printing	Font Management	All Settings
Universal Scanning	Scanning Applications	All Settings
Connection	Authentication	All Settings
Connection	Second Level Authentication	All Settings
Connection	Allowed Devices	All Settings
Reporting	Reporting Engine	Reporting Engine Type
Reporting	Engine specific settings	All Settings

To replicate a specific setting to all other sites, tick the option **Replicate settings** highlighted in the below screenshot.



Enabling Replication of Configuration Changes to all other Sites

Overriding Site Replicated Settings

If an administrator has permissions to enable or disable the replication settings makes a change to a specific setting, such setting is replicated to all other sites.

If an administrator has access to a particular site only, upon modifying site settings which have been replicated, the replicated settings are overridden and the option **Replicate Settings** is automatically switched off, therefore such settings will no longer be replicated to other sites.

Setting a Site as a Licensing Server

If the licensing server fails, or if you would like to set a different site as a Licensing Server, click on the site's name from the **Farm** node in the navigation tree, and from the **Tasks** drop down menu select **Set Site as Licensing Server**.

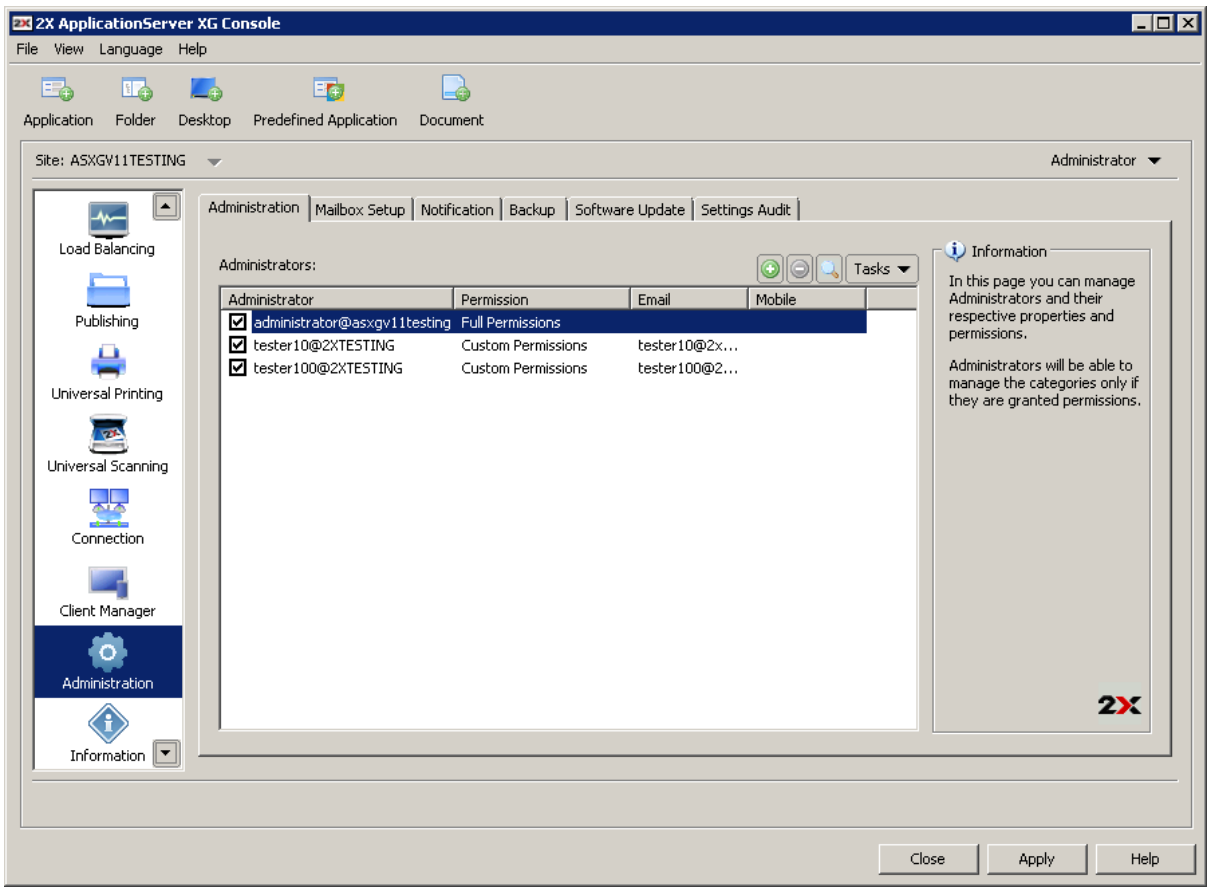
Administrators

Introduction

It is possible to have multiple 2X ApplicationServer XG administrators that can manage and configure the farm and sites within the farm. Permissions can also be configured to limit access to specific categories and Sites.

If the 2X ApplicationServer XG is installed in an Active Directory environment, any user that has elevated privileges and write access to the installation directory can be configured as a 2X ApplicationServer XG administrator.

If the 2X ApplicationServer XG is installed on a standalone machine, any user that has elevated privileges and write access to the installation directory can be configured as a 2X ApplicationServer XG administrator.



Managing Administrators from the Administration Category

Default 2X ApplicationServer XG Administrator

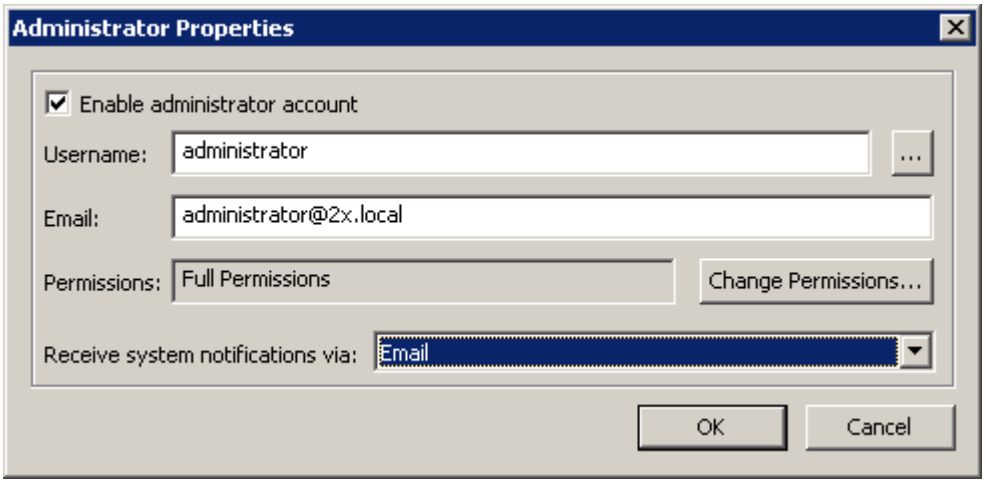
The user you specified the first time to login to the 2X ApplicationServer XG Console will automatically have full permissions and can perform any task in the farm. There should always be at least one enabled administrator with full permissions in the farm.

Adding an Administrator Account

To add an administrator account to the 2X ApplicationServer XG follow the below procedure:

1. Access the **Administration** category and click the **Administration** tab.
2. From the **Tasks** drop down menu select **Add**.

3. Specify a username in the **Username** field or click the **browse** button to select a user from the active directory or local machine in the **Administrator Properties** dialog box.



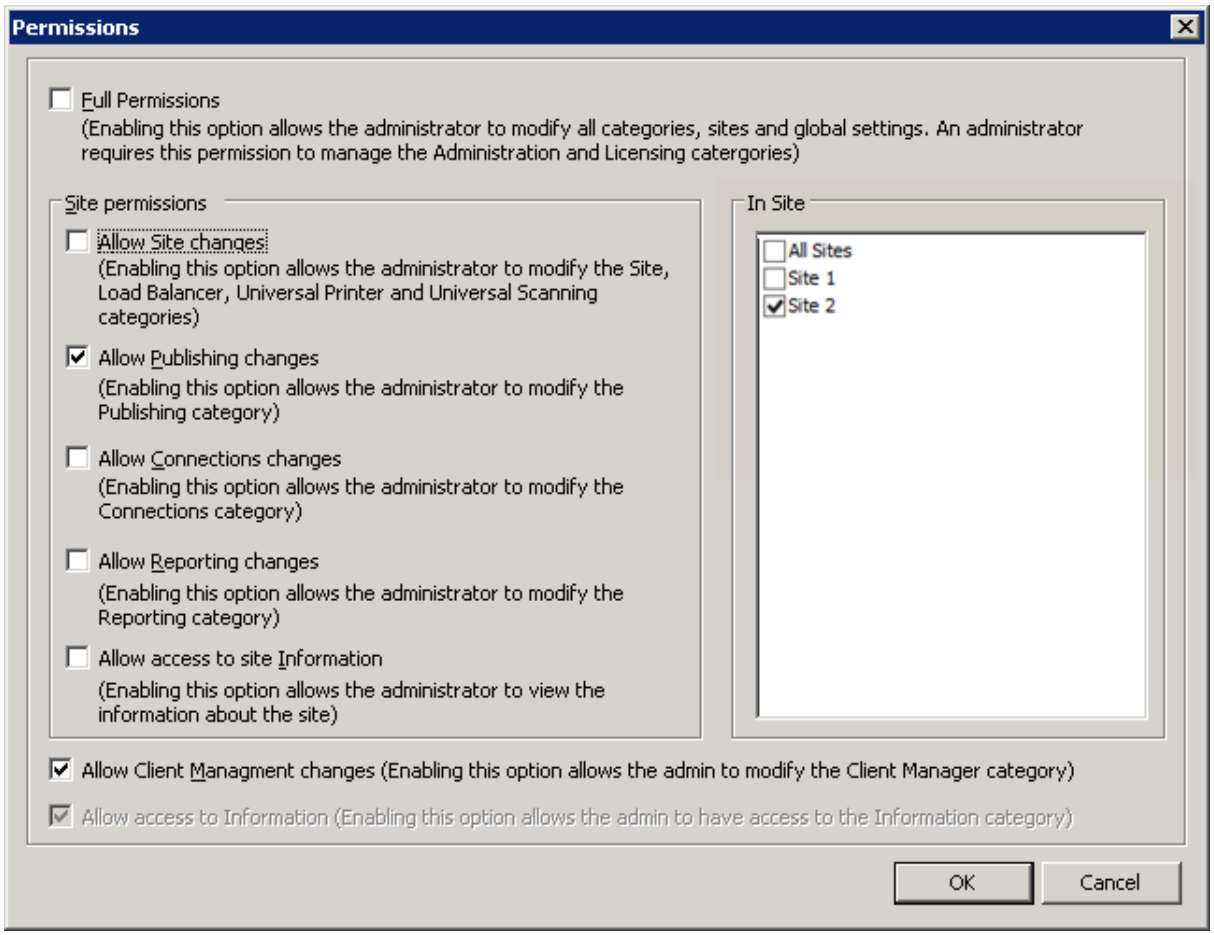
Configuring a New 2X ApplicationServer XG Administrator

4. Specify an email address in the **Email** input field.
5. By default the new Administrator account will be assigned full permissions. Click the **Change Permissions** button to modify the permissions. For more information on administrators permissions, refer to the section **Configuring Administrator Accounts Permissions** below.
6. From the **Receive system notifications via** drop down menu select **Email** so any system notifications are sent to the specified email address. Select **None** to disable email system notifications for this account.
7. Click **OK** to add the new administrator account.

Configuring Administrator Accounts Permissions

Administrator permissions can be configured when creating a new administrator account or from the **Properties** of an existing account.

Permissions can be assigned per category (e.g. Farm, Publishing, Universal Printing etc) and also per site as seen in the below screenshot.


Permissions
Full Permissions
(Enabling this option allows the administrator to modify all categories, sites and global settings. An administrator requires this permission to manage the Administration and Licensing catergories)
Site permissions
Allow Site changes
(Enabling this option allows the administrator to modify the Site, Load Balancer, Universal Printer and Universal Scanning categories)
Allow Publishing changes
(Enabling this option allows the administrator to modify the Publishing category)
Allow Connections changes
(Enabling this option allows the administrator to modify the Connections category)
Allow Reporting changes
(Enabling this option allows the administrator to modify the Reporting category)
Allow access to site Information
(Enabling this option allows the administrator to view the information about the site)
In Site
All Sites
Site 1
Site 2
Allow Client Managment changes (Enabling this option allows the admin to modify the Client Manager category)
Allow access to Information (Enabling this option allows the admin to have access to the Information category)
OK
Cancel

Configuring 2X ApplicationServer XG Administrator Permissions

An account with **Full Permissions** can modify all categories, sites and global settings in the farm.

Permissions Example

To allow an administrator to manage and configure publishing and published objects on Site 2, disable all permissions except the Allow Publishing changes option and tick Site 2 as seen in the above screenshot.

Managing Administrator Accounts

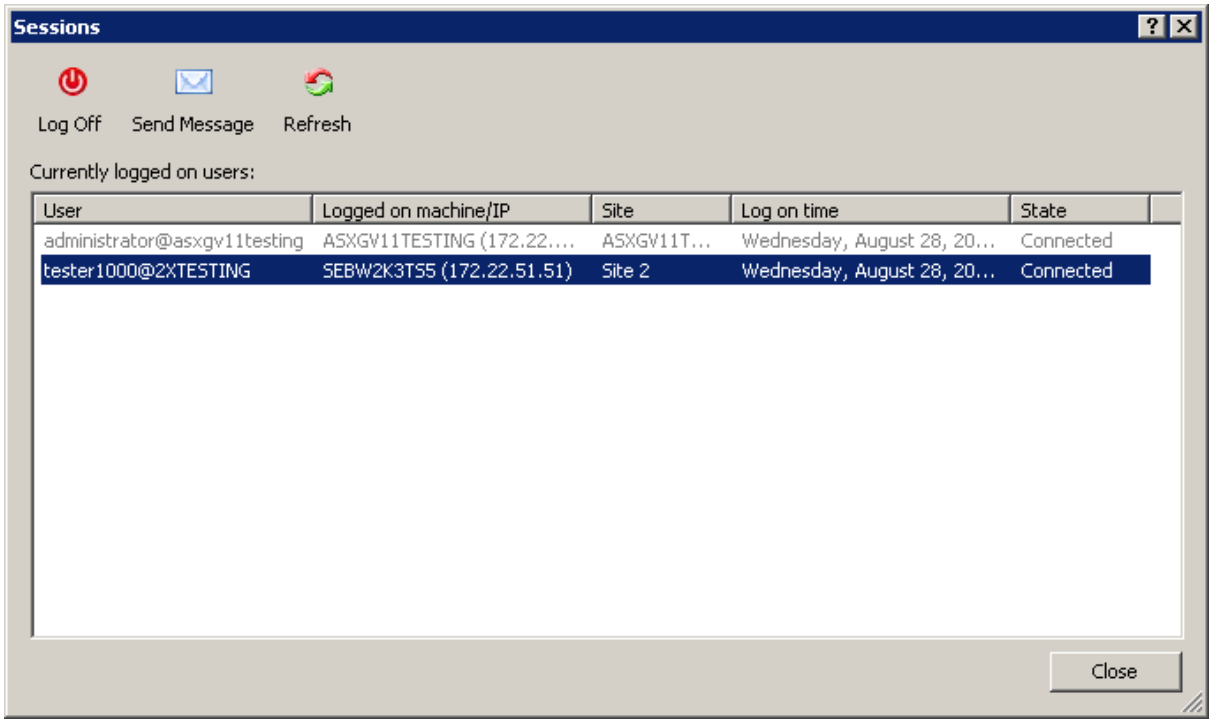
From the **Administration** tab in the **Administration** category you can add new administrator accounts and modify or delete existing ones.

Sending Console Messages between Administrator Accounts

If multiple administrators are logged in to the 2X ApplicationServer XG console, they can send messages to each other. To send message to another logged in administrator click the arrow next to your account name (top right corner) in the 2X ApplicationServer XG Console and select **Send Message** from the drop down menu.

Note: the same administrator may be logged in more than one session.

From the **Sessions** dialog box highlight the account and click **Send Message**.

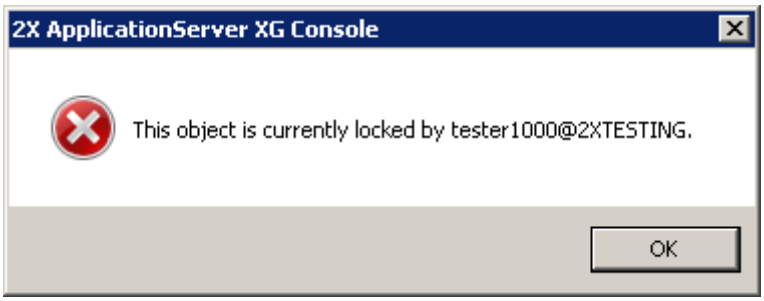


Sessions Dialog Box Lists all Currently Logged in Administrators

Note: Messages between administrators are not archived or recorded.

Logging off Other Administrators

When an administrator is accessing a category, for example Universal Printing, it will be locked for all other administrators. Therefore upon trying to access a category locked by another administrator, the administrator will be alerted with an error that the object is locked.



Alert Generated when a Category is Locked by another Administrator

To log off an administrator from locking a category, navigate to the **Administration** category, and from the **Administration** tab click the **Tasks** drop down menu and select **Show Sessions**. From the sessions dialog box you can send messages to other administrators or log them off from their 2X ApplicationServer XG Console session.

Terminal Servers

Introduction

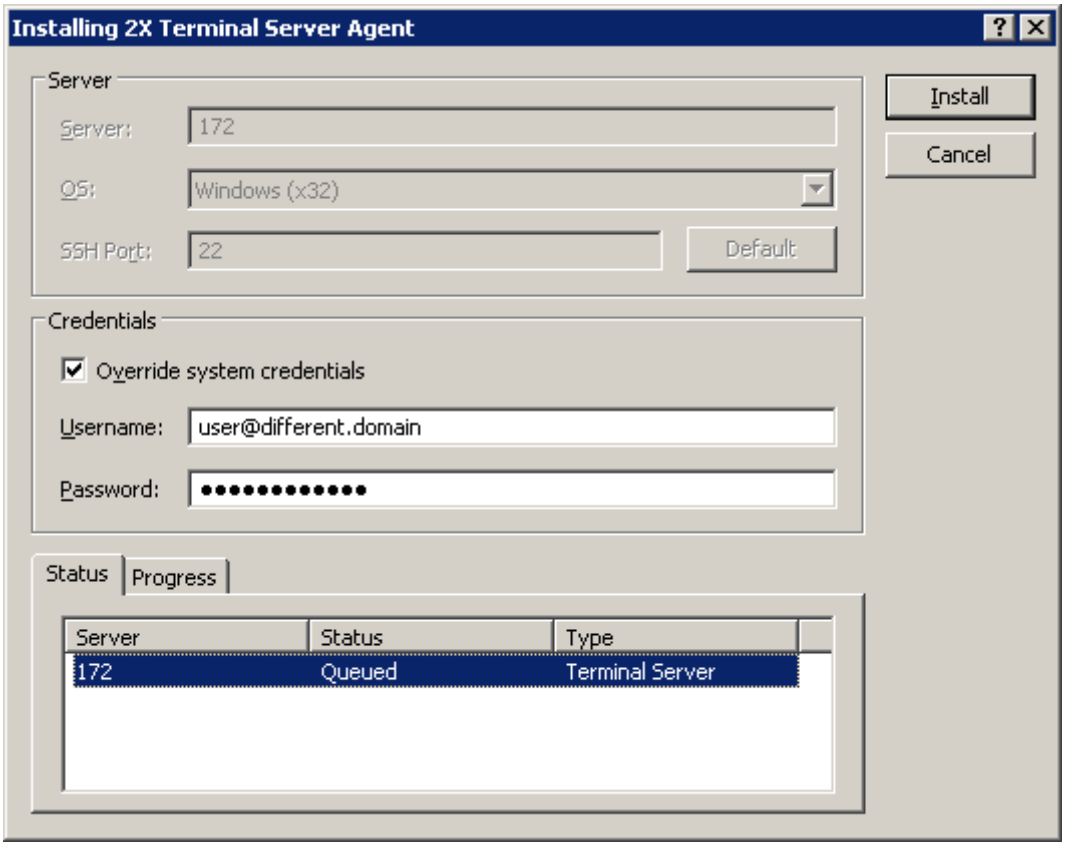
To be able to publish Applications and Desktops for your users through 2X ApplicationServer XG first you need to add a server to the farm. This chapter explains how to add and manage a Terminal Server in the farm.

Adding a Terminal Server

Requirement: To add a terminal server to the farm it must have the Remote Desktop Services installed.

Follow the below procedure to add a Terminal Server to the farm:

1. Launch the 2X ApplicationServer Console, select the **Farm** category and click on **Terminal Servers** from the navigational tree.
2. Click **Add** from the **Tasks** drop down menu to launch the setup wizard and once prompted specify the server IP address or FQDN and click **Next**.
3. In this step the 2X ApplicationServer XG checks if the 2X agent is installed on the Terminal Server. If it is installed, proceed to step 7 of this procedure. If it is not installed, click **Install** to remotely install the 2X Agent.
4. In the **Installing 2X Terminal Server Agent** dialog highlight the server name on which the 2X Agent is to be installed.
5. (Optional) Tick the option “Override system credentials” to specify and use different credentials to connect to the server and install the 2X Agent as seen in the below screenshot.



Specifying Different Credentials to Install 2X Terminal Server Agent

6. Click **Install** to install the agent and click **Done** once it has been successfully installed. If the automatic installation of the 2X Agent fails refer to the following section **Installing the 2X Terminal Server Agent Manually**.
7. Click **Add** to add the Terminal Server to the 2X ApplicationServer XG farm.

Tip: Use the **Find** option from the **Tasks** drop down menu to find existing terminal servers in your active directory domain.

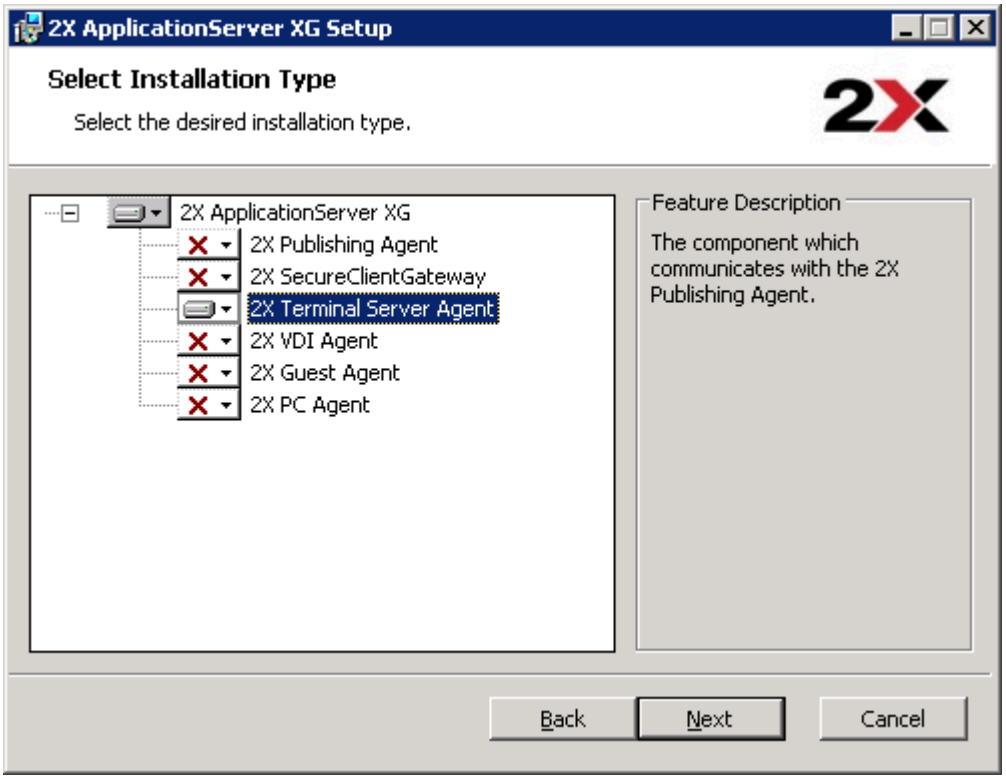
Installing the 2X Terminal Server Agent Manually

2X Terminal Server Agent System Requirements

- Windows 2003 SP1 Server or 2008 Server or Advanced Server with Remote Desktop Services enabled.
- The same hardware requirements as specified by Microsoft when deploying a Remote Desktop Services environment will apply.

Installing the 2X Terminal Server Agent Manually

1. Login to the server where the 2X Terminal Server Agent is to be installed using an administrator account and close all other applications.
2. Copy the 2X ApplicationServer installation file (2XAppServer.msi) to the server and double click it to launch the installation.
3. Once prompted click **Next** and accept the End-User license agreement.
4. Specify the path where the 2X Agent should be installed and click **Next**.
5. Select **Custom** and click **Next**.
6. Click on the **2X Terminal Server Agent** and select **Entire Feature will be installed on local hard drive** from the drop down menu as seen from the below screenshot.



Manually installing a Terminal Server Agent

7. Ensure that all other components are deselected and click **Next**.
8. Click **Install** to start the installation and **Finish** once the installation is finished.

Note: The 2X Agent does not require any configuration. Once the 2X Agent is installed, highlight the server name in the 2X ApplicationServer Console and click **Check Agent**. If the agent is installed properly, the status should change to **Agent Installed** as seen in the below screenshot.

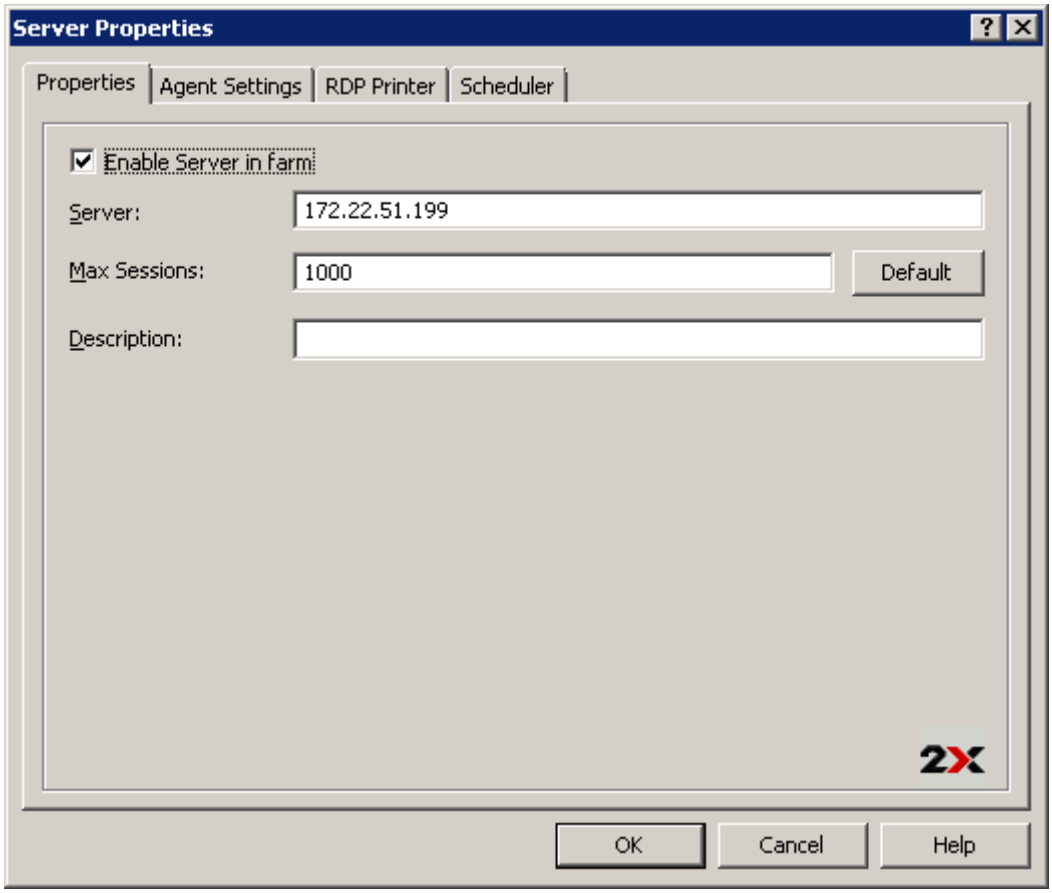
Configuring a Terminal Server

To access the properties of a Terminal Server highlight the server from the navigation tree in the 2X ApplicationServer Console and select **Properties** from the **Tasks** drop down menu. All of the below configuration options can be configured from the **Server Properties**.

Enabling or Disabling a Terminal Servers

By default a server is enabled in the farm. When it is disabled, published applications and virtual desktops cannot be served from it.

To disable a server from the farm untick the option **Enable Server in farm** from the **Properties** tab in the **Server Properties**. Tick back (enable) any of the tick boxes to enable the server back in the farm.



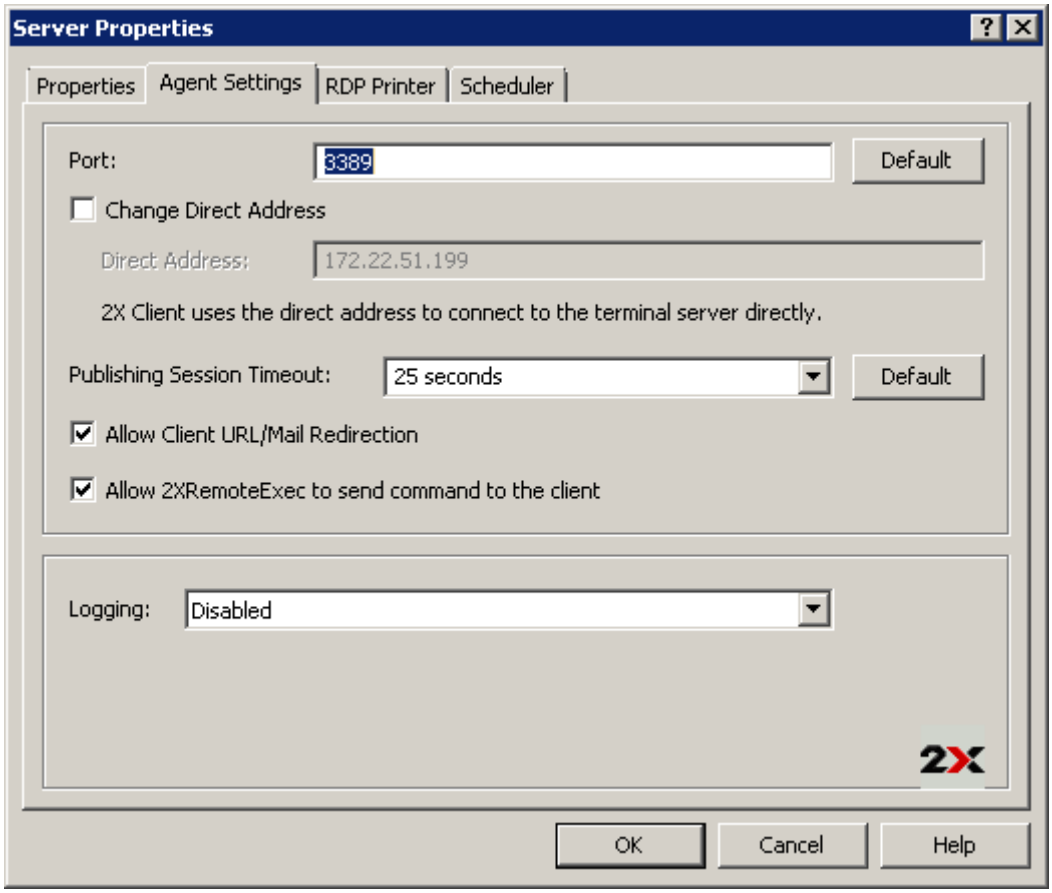
Properties Tab in Server Properties

Configuring Server Name and Maximum Sessions

From the **Properties** tab shown in the above screenshot you can also configure the server name, maximum number of sessions allowed to connect to the server simultaneously and the server description.

Configuring the 2X Terminal Server Agent on the Server

Each Terminal Server in the farm has a 2X Agent installed to provide a connection between the 2X ApplicationServer XG and the Terminal Server. The agent can be configured from the **Agent Settings** tab in the server properties.



Configuring Terminal Server Agent from the Agent Settings Tab in Server Properties

Configuring the Remote Desktop Connection Port

Specify a different remote desktop connection port number in the **Port** input field if a non default port is configured on the server.

Changing the Direct Address

This address is only used in Direct Connection mode and it could be an internal or external IP address. To change the Direct Address of a server tick the option **Change Direct Address** and specify the new address in the **Direct Address** input field.

Changing the Session Timeout

To change the amount of time each session remains connected in the background after the user has closed the published application specify a new value in the **Publishing Session Timeout** input field. This option is used to avoid unnecessary reconnections with the server.

Configuring URL and Mail Redirect / Restricting Access

To allow http and mailto links to be opened using a local application on the client computer rather than the server's resources, enable the option **Allow Client URL/Mail Redirection**. To configure a list of URLs which should not be redirected navigate to the **URL Redirection** tab in the **Settings** node of a site.

Allow 2XRemoteExec to send commands to client

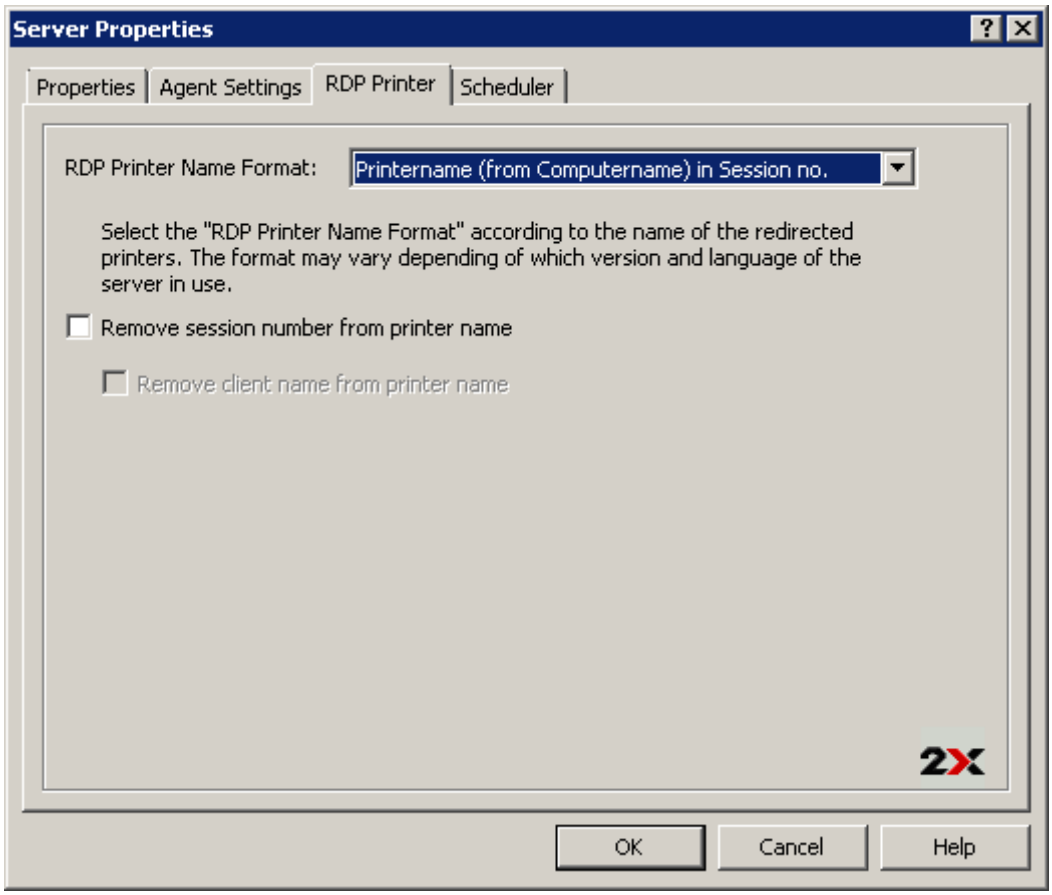
To allow a process which is running on the server to instruct the client to deploy an application on the client side, enable this option. For more information about 2XRemoteExec refer to the following blog post; http://www.2x.com/blog/2012/11/tech/new-feature-in-applicationserver-xg-v10-5-server-to-client-commands/.

Configuring 2X Terminal Server Agent Logging

To enable or disable the 2X Terminal Server Agent logging use the **Logging** drop down menu. Such logging should only be enabled if instructed by the 2X support team.

Configuring RDP Printing for Terminal Server

The **RDP Printer** tab allows you to configure the renaming format of redirected printers. The format may vary depending of which version and language of the server you are using.


Server Properties
Properties
Agent Settings
RDP Printer
Scheduler
RDP Printer Name Format:
Printername (from Computername) in Session no.
Select the "RDP Printer Name Format" according to the name of the redirected printers. The format may vary depending of which version and language of the server in use.
Remove session number from printer name
Remove client name from printer name
2X
OK
Cancel
Help

Configuring RDP Printers from the RDP Printer Tab in Server Properties

Set your RDP Printer Name Format specifically for the configured server by choosing any of the below options from the **RDP Printer Name Format** drop down menu:

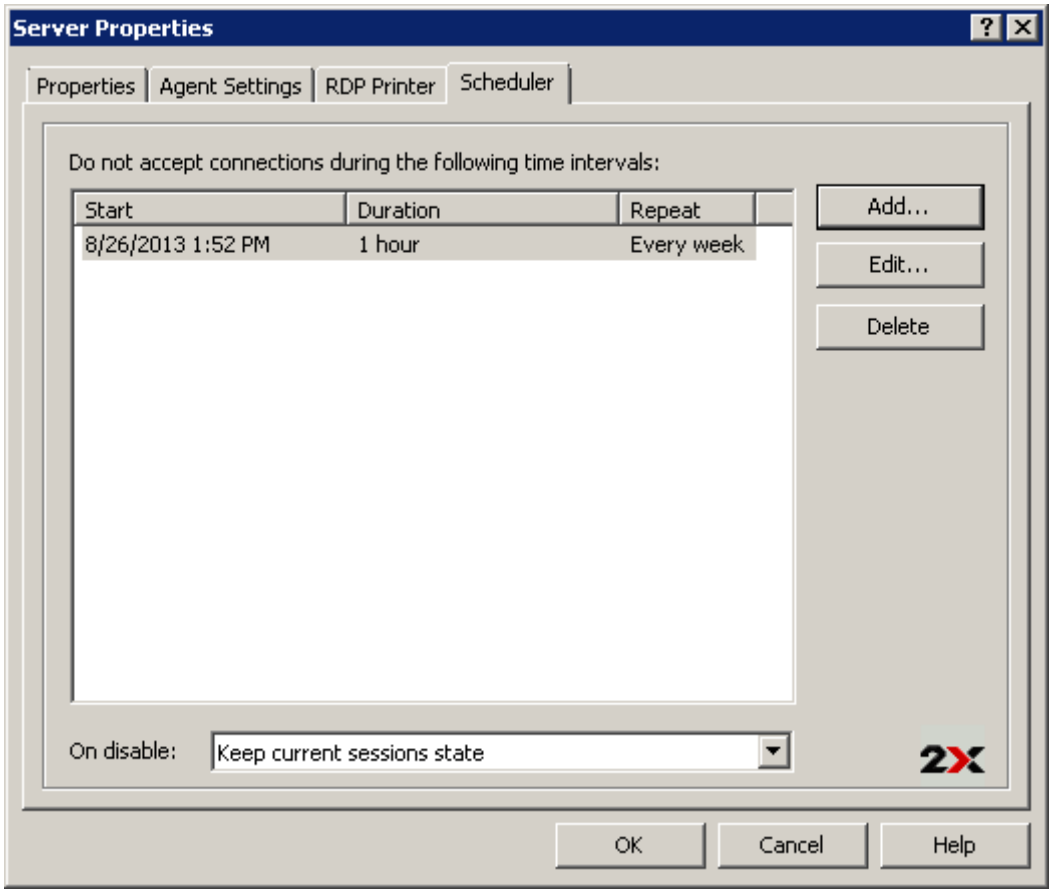
- Printername (from Computername) in Session no.
- Session no. (computername from) Printername
- Printername (redirected Session no.)

The other RDP Printing options available in the RDP Printer tab are:

- Remove session number from printer name
- Remove client name from printer name

Configuring Terminal Server Maintenance Time Window

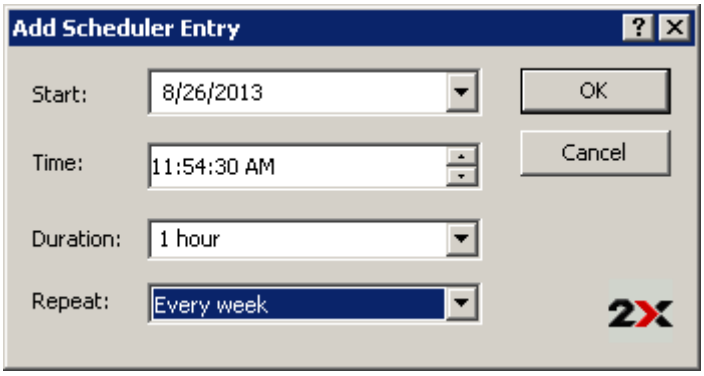
From the **Scheduler** tab in the server properties you can create and configure a maintenance time window for the server. During a maintenance window published resources won't be accessible from that server. Current active sessions can be left running, disconnected or even reset.



Configuring Maintenance Time Window from the Scheduler Tab in Server Properties

To configure a maintenance time window click the **Add** button to configure the:

- Start date
- Time
- Duration
- Repeat: from this option configure the repeat interval of the maintenance time window, for example every week, month etc.



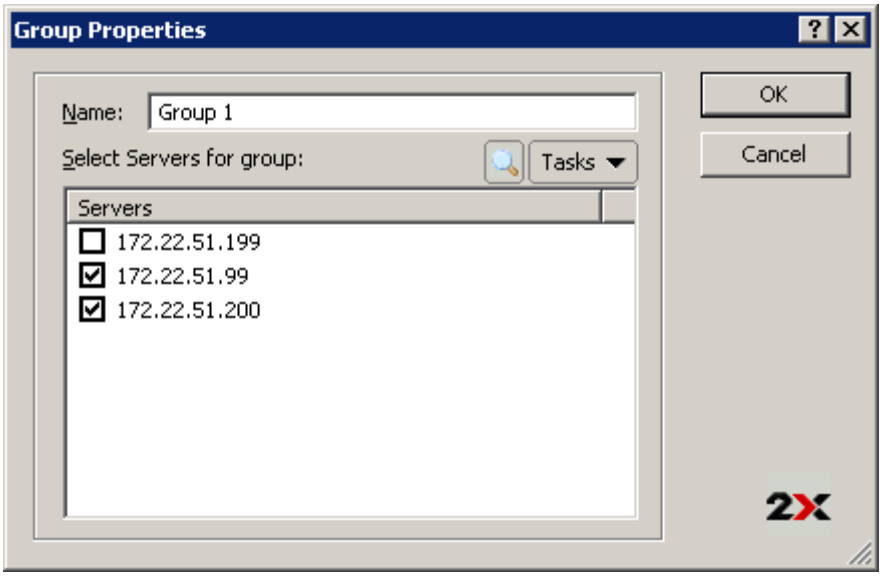
Configuring a New Maintenance Time Window

Once you configure the time for the maintenance window, use the drop down menu **On Disable** at the bottom of the **Scheduler** tab to specify what happens of the current sessions once the server has been disabled for maintenance.

Grouping Terminal Servers

Terminal Servers groups can be used to specify from which group of servers a published resource should be published in the wizard. It is highly recommended to use groups in a multi-server environment to ease the management of publishing items.

Click the **Groups** tab in the **Terminal Servers** section to create and manage terminal servers groups. Click **Add** from the **Tasks** drop down menu to create a new terminal server group, or **Properties** to modify an existing terminal server group and **Delete** to delete the highlighted terminal server group.

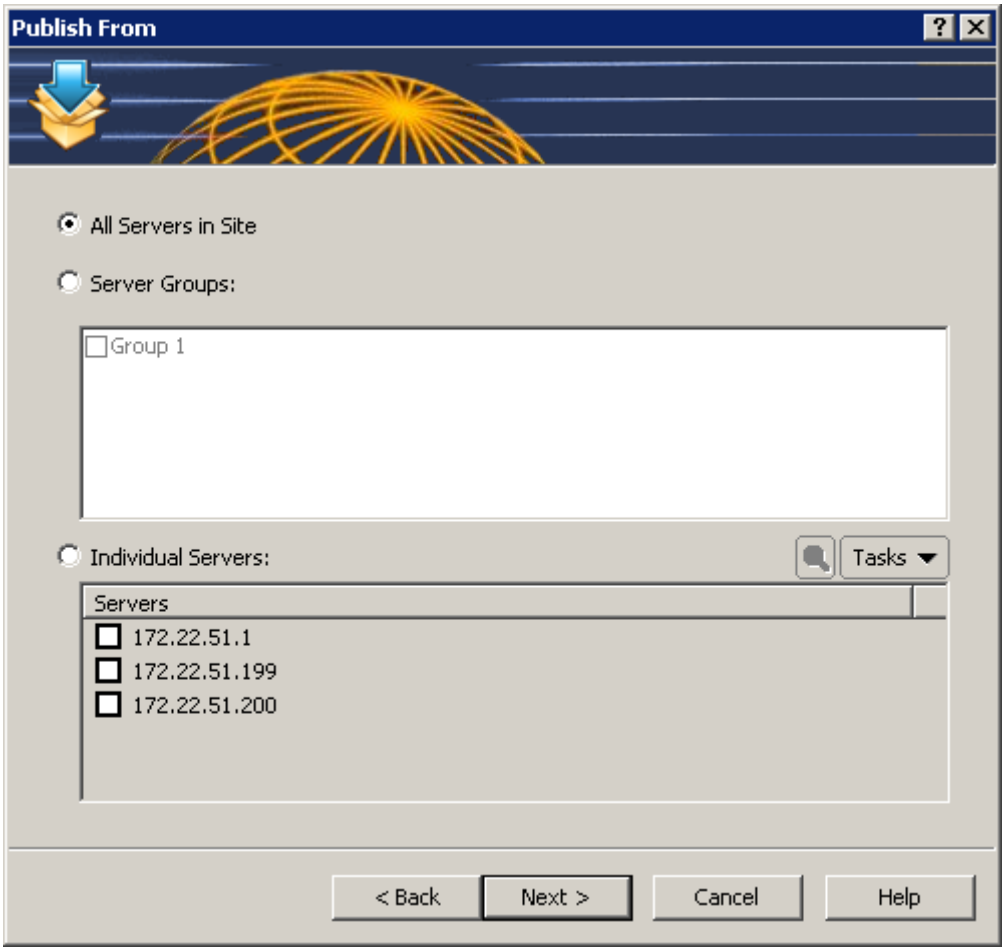


Configuring a New Terminal Servers Group

Publishing a Desktop from a Terminal Server

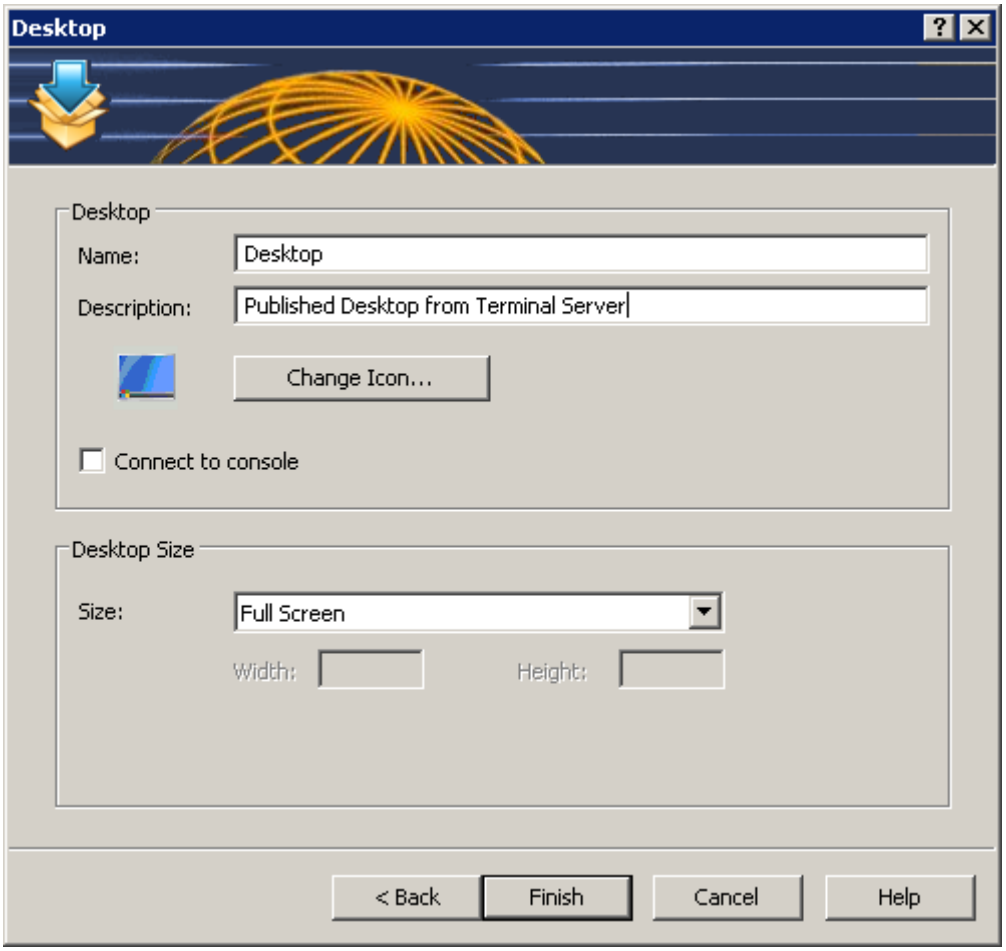
To publish a desktop from a terminal server follow the below procedure:

1. Select the **Publishing** category and click the **Desktop** icon from the top navigation bar to launch the desktop publishing wizard.
2. Select **Terminal Server Desktop** in the first step of the wizard and click **Next**.
3. In the second step of the wizard specify from which Terminal Servers the desktop should be published. You can specify to publish the desktop from **All Servers in Farm**, **Server Group/s** or from a number of **Individual Servers** as seen in the below screenshot.



Selecting Terminal Servers from Where to Publish a Desktop

4. In the third step of the wizard specify a **Name** and **Description** in the **Desktop** section. From the same section you can also configure a different icon by clicking on the **Change Icon** button. Tick the option **Connect to console** so users connecting to the published desktops will connect to the terminal server's console rather than a virtual desktop session.
5. From the **Desktop Size** section you can also specify the resolution of the desktop.



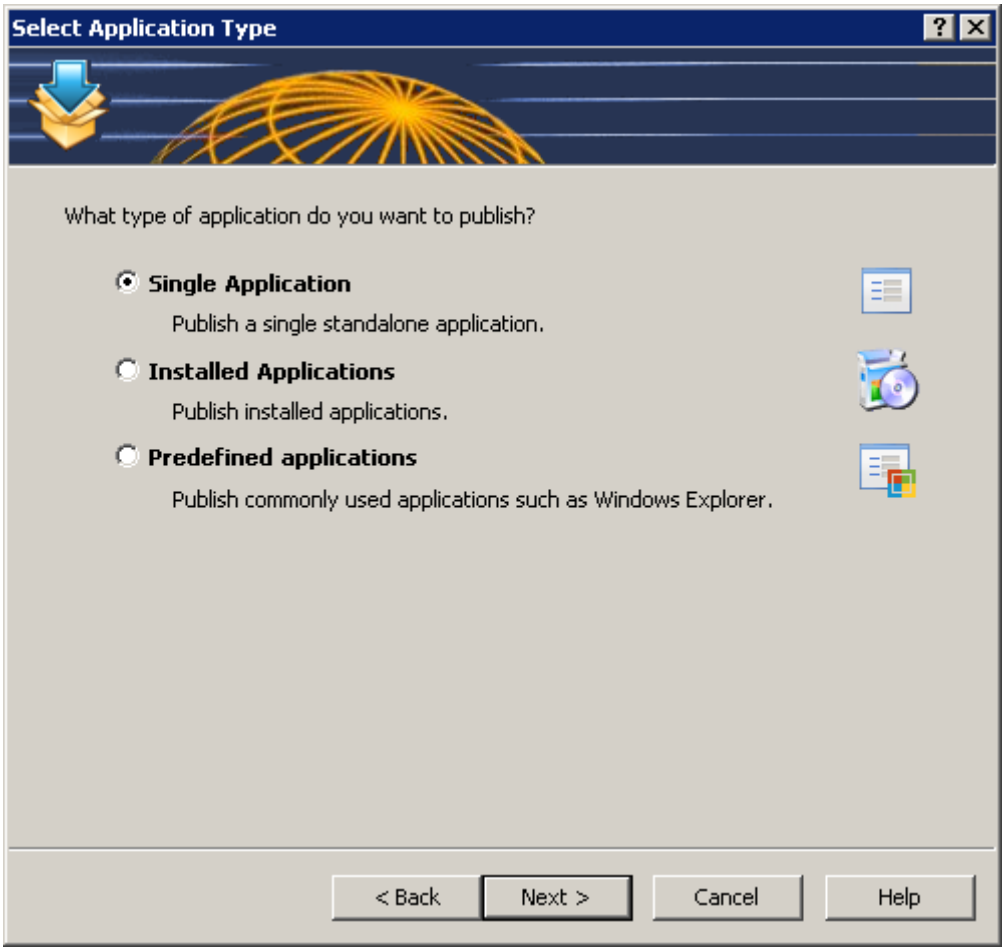
Configuring a desktop to be published from a Terminal Server

6. Click **Finish** to publish the desktop.

Publishing an Application from a Terminal Server

To publish an application from a terminal server follow the below procedure:

1. Open the **Publishing** category and click the **Application** icon from the top navigation bar.
2. Select **Terminal Server** in the first step of the wizard and click **Next**.
3. In the second step of the wizard, select the type of application to be published. The options are:
    a. **Single Application**: Choose this option to fully configure the application settings yourself such as the executable path etc.
    b. **Installed Application**: Choose this option to publish an application that is already installed on the server therefore all of the application settings are automatically configured.
    c. **Predefined Application**: Choose this option to publish a commonly used Windows application such as Windows Explorer.



Selecting an Application Type from the Publish an Application Wizard

4. In the third step of the wizard specify from which Terminal Servers the application should be published. You can specify to publish the desktop from **All Servers in Farm**, **Server Group/s** or from a number of **Individual Servers**.
5. If you selected **Installed Application** or **Predefined Application** in the fourth step of the wizard you have to select the application to be published by ticking the application name and click **Finish** to publish the application. If you selected **Single Application** you have to configure the application as explained in the following procedure:

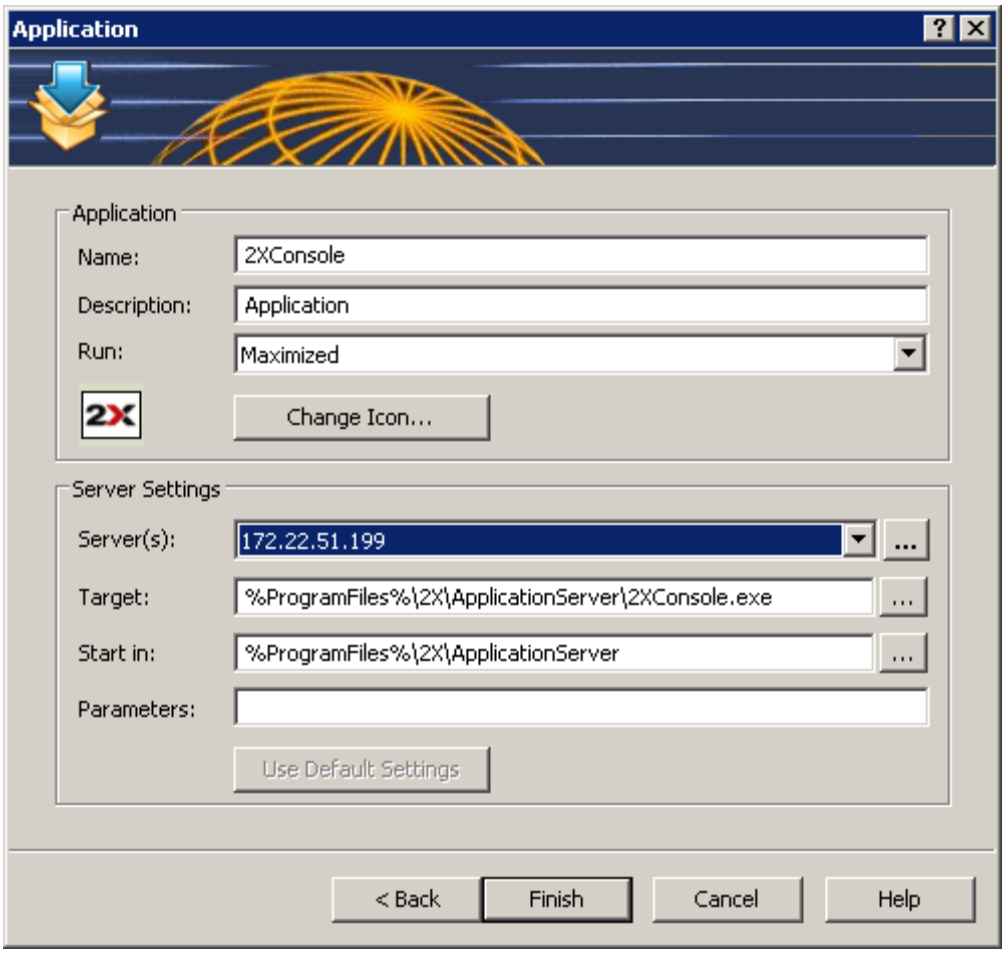
Configuring a Single Application

Note: By browsing to an application using the the **Browse** button next to the **Target** input filed all entries will be automatically populated. Else follow the below procedure to populate all fields manually.

6. Enter a **Name** and **Description** in the **Application** section and from the Run drop down menu specify if the application should run in a normal window, maximized or minimized.
7. (Optional) You can change the icon for the published application by clicking the **Change Icon** button.
8. Specify the path where the application executable is in the **Target** input field by clicking the **browse** button and browse to the executable. Use Windows environment variables if you are manually specifying the path.
9. The **Start In** input field will be automatically populated. To specify a different folder from where the application should be launched click the **Browse** button. A different folder might be specified if for example the application needs to use files from another

location to run. In such case, specify such folder location so the published application will be able to locate them upon it being launched.

10. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application upon being launched.



Configuring a New Application to be Published from a Terminal Server

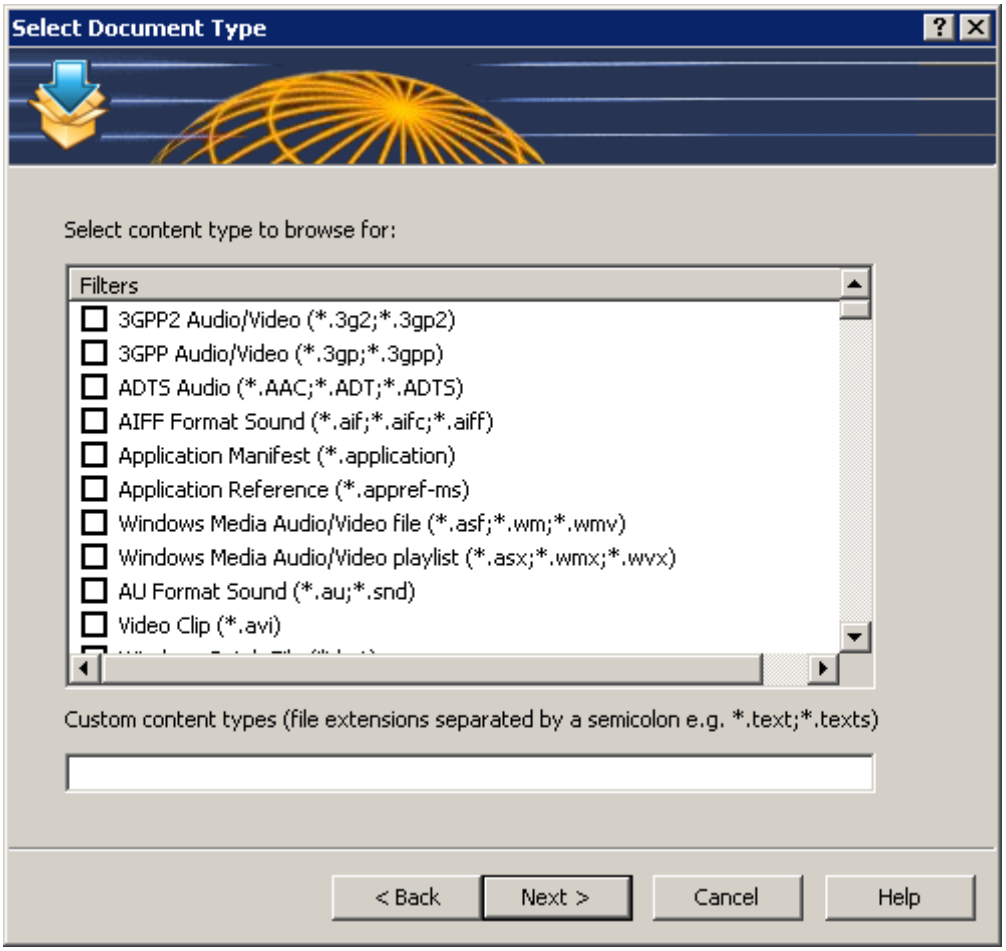
Note: Use the **Server(s)** drop down menu to specify different application settings for a specific server in case the application is installed in a different path on that particular server.

11. Once the application is configured click **Finish** to publish the application.

Publishing a Document from a Terminal Server

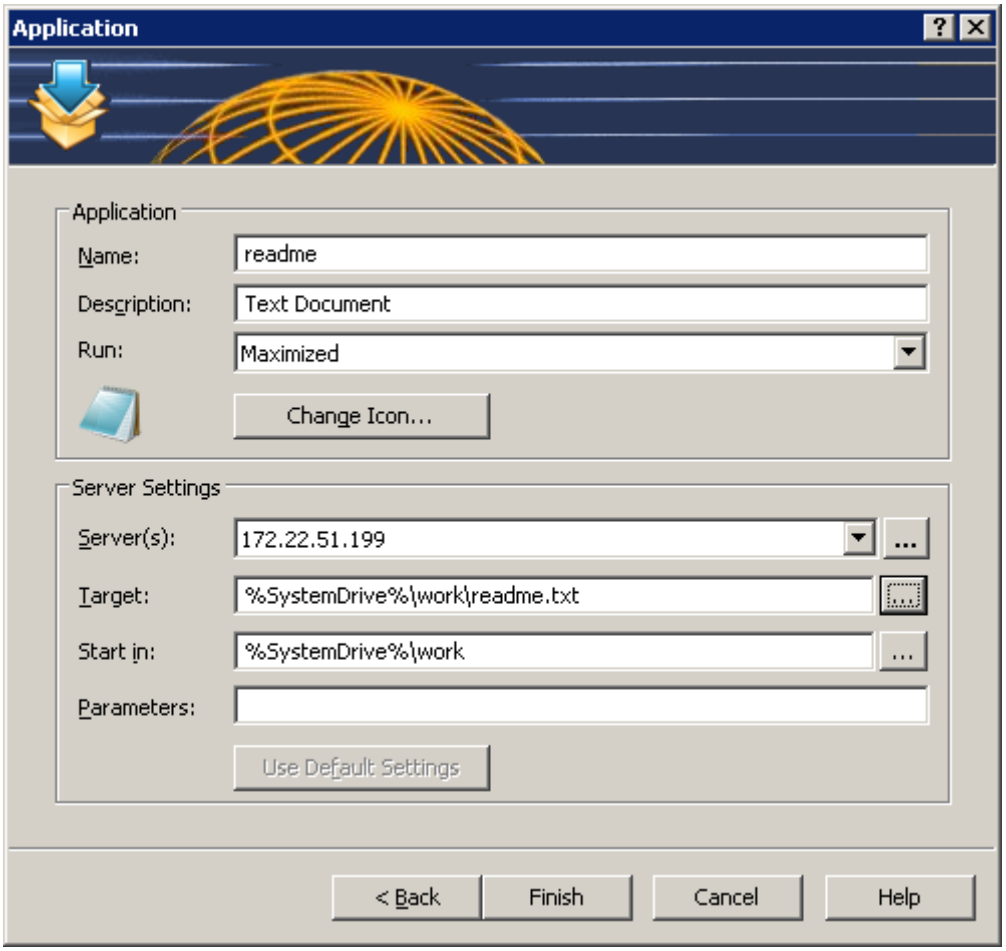
To publish a document from a terminal server follow the below procedure:

1. Select the **Publishing** category and click the **Document** icon from the top navigation bar.
2. Select **Terminal Server** in the first step of the wizard and click **Next**.
3. In the second step specify the content type of the document you want to publish. You can select the content type from the predefined list or specify a custom content type from the **Custom content types** input field. Click **Next** once ready.



Configuring a Content Type for the Document

4. In the third step of the wizard specify from which Terminal Servers the document should be published. You can specify to publish the desktop from **All Servers in Farm**, **Server Group/s** or from a number of **Individual Servers**.
5. In the fourth step of the wizard, use the **Browse** button next to the **Target** input field to browse to the document. All other fields will be automatically populated. To edit any of the auto populated fields highlight them and enter the required details.
6. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application running the document upon being started.



Configuring the Document to be Published from a Terminal Server

Note: Use the **Server(s)** drop down menu to specify different document settings for a specific server in case the document is configured differently on that particular server.

7. Once ready click **Next** and configure the filtering options. For more information about filtering options refer to the Filtering section on page 86.
8. Click **Finish** to publish the document.

VDI Hosts

Introduction

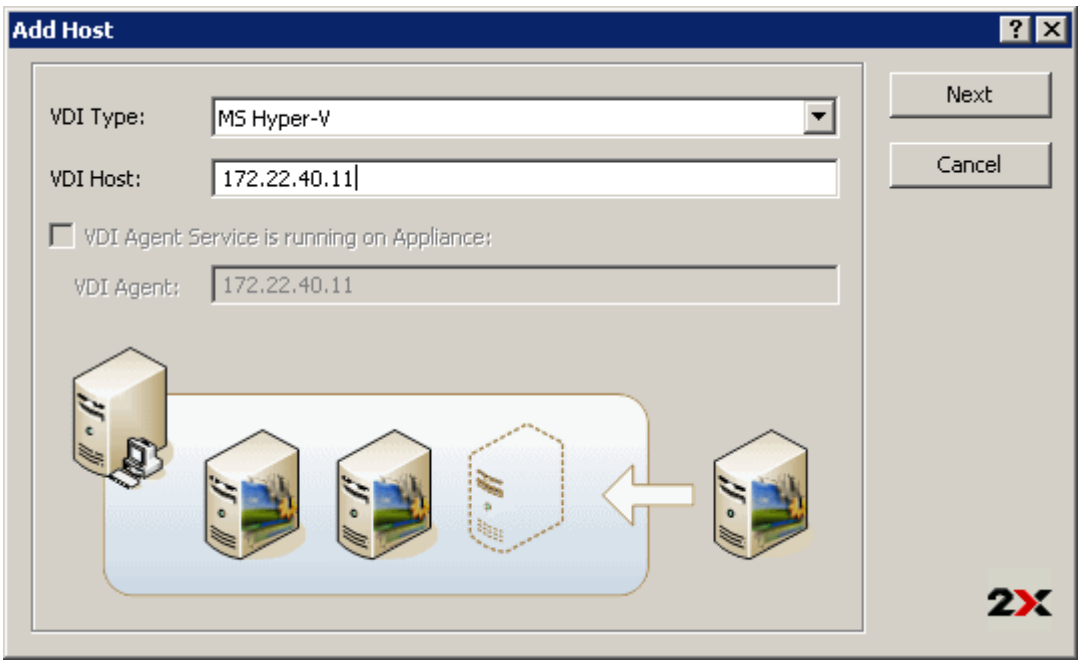
A VDI Host (**host machine**) is defined as the computer on which a hypervisor is running one or more virtual machines. Each virtual machine is called a **guest machine**. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources.

By adding the VDI Host to the 2X Application Server you can manage the virtual machines on the VDI Host, create guest clones and publish virtual desktops and applications from virtual guests.

Adding a VDI Host

For a complete list of supported VDI Hosts please refer to the online list of approved Hypervisors; http://www.2x.com/applicationserver/approved-vdi. To add a VDI Host to the farm follow the below procedure:

1. Launch the 2X ApplicationServer Console, click the **Farm** category and click on **VDI Hosts** node of the site where you would like to add the hypervisor.
2. Click **Add** from the **Tasks** drop down menu to launch the setup wizard and once prompted select the type of VDI from the **VDI Type** drop down menu.



Adding a VDI Host

3. Specify the IP address or FQDN of the VDI Host and click **Next** (Refer to the **note** below for more information about configuring the VDI Agent for some of the hypervisors).
4. In this step the 2X ApplicationServer XG checks if the 2X VDI agent is installed on the VDI Host. If it is installed, proceed to step 8 of this procedure. If it is not installed, click **Install** to remotely install the 2X agent.
5. In the **Installing 2X VDI Host Agent** dialogue highlight the server name on which the 2X Agent is to be installed.
6. (Optional) Tick the option "Override system credentials" to specify and use different credentials to connect to the server and install the 2X Agent.
7. Click **Install** to install the agent and click **Done** once it has been successfully installed. If the automatic installation of the 2X Agent fails refer to the following section **Installing the 2X VDI Agent Manually**.
8. Click **Add** to add the VDI Host to the 2X ApplicationServer server farm.

Note: To add some of the supported hypervisors different steps and procedures must be followed, such as installing the 2X VDI Agent appliance on the hypervisor server. Before adding a hypervisor server to the farm, refer to the hypervisor manuals which are available in the 2X documents page; http://www.2x.com/documentation/. All hypervisors manuals are available under the **Supported VDI Hypervisors** section.

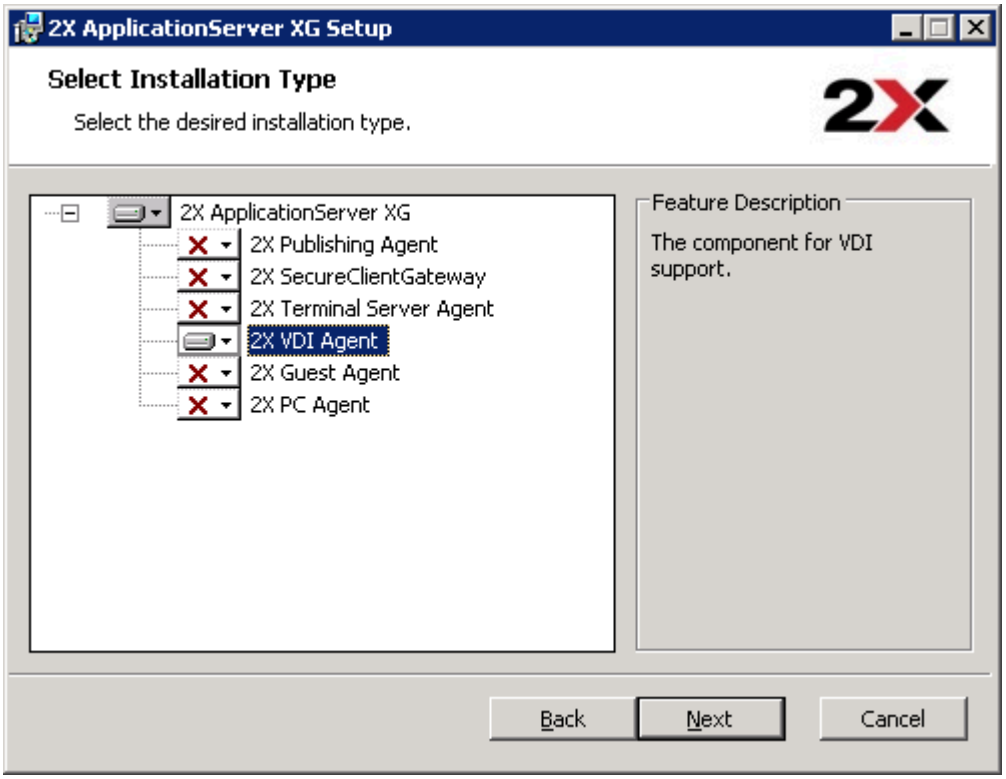
Installing the 2X VDI Agent Manually

2X VDI Agent System Requirements

- Windows XP, Windows Vista, Windows 2000 Server, Windows 2003 Server or Windows 2008 Server or Advanced Server.
- The same hardware requirements as specified by your virtualization software will apply.
- One of the supported virtualization software technology:
  - If you are planning to use VMware on Windows, make sure the VMware VmCOM Scripting API is installed. The following error will be displayed if VmCOM Scripting API is not detected: "VMware VmCom Scripting API is not installed on the host. Please install this client component from the VMware installer."
  - If you are planning to use VMware v1.* on Linux, make sure the VMware VIX API for Linux is installed. The following error will be displayed if VIX API for Linux is not detected: "VMware VIX API for Linux is not installed on this host. Please download this component from http://www.vmware.com"
  - If you are planning to use Virtual Iron, make sure that you install Java Runtime Environment on the same machine where 2X VDI Agent is installed.

Installing the 2X VDI Agent Manually

1. Login to the server where the 2X VDI Agent is to be installed using an administrator account and close all other applications.
2. Copy the 2X ApplicationServer installation file (2XAppServer.msi) to the server and double click it to launch the installation.
3. Once prompted click **Next** and accept the End-User license agreement.
4. Specify the path where the 2X Agent should be installed and click **Next**.
5. Select **Custom** and click **Next**.
6. Click on the 2X VDI Agent and select **Entire Feature will be installed on local hard drive** from the drop down menu as seen in the below screenshot.



Manually Installing the VDI Agent

7. Ensure that all other components are deselected and click **Next**.
8. Click **Install** to start the installation and **Finish** once the installation is finished.

Note: The 2X Agent does not require any configuration. Once the 2X Agent is installed, highlight the server name in the 2X ApplicationServer console and click **Check Agent**. If the agent is installed properly, the status should change to **Agent Installed** as seen in the below screenshot.

Installing an Appliance

Introduction

For some of the Hypervisors such as VMWare ESXi server, you have to configure and run an appliance instead of the 2X agent. An appliance is a pre-configured virtual machine (including the operating system and other relevant settings) which you can add to the list of virtual machines running on the hypervisor to act as a 2X Agent.

Installing the Appliance

To install an appliance on a hypervisor refer to the hypervisor's documentation found in the 2X documentation page; http://www.2x.com/documentation/.

Configuring a VDI Host

To access the properties of a VDI Host highlight the server from the navigation tree in the 2X ApplicationServer Console and select **Properties** from the **Tasks** drop down menu. All of the below configuration options can be configured from the **Server Properties**.

Note: Some of the settings mentioned below might be unavailable out for some servers. This depends on the type of hypervisor server being used.

Enabling or Disabling a VDI Servers in the Farm

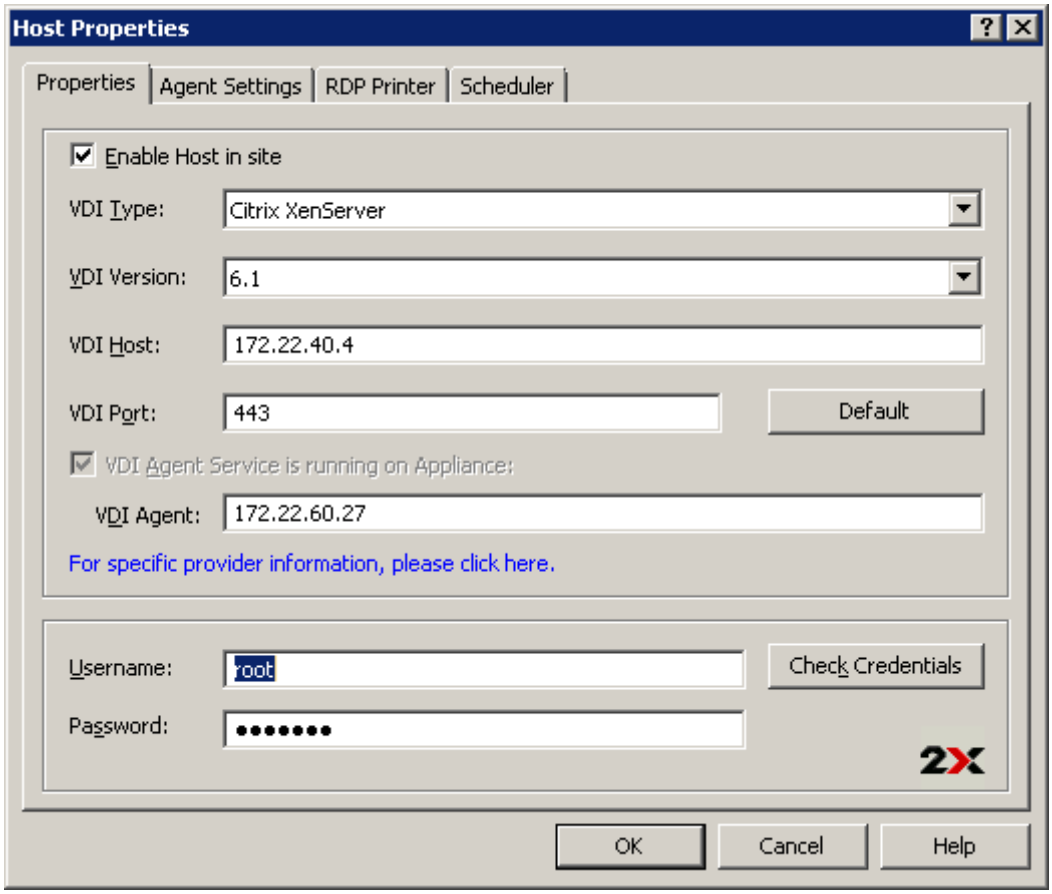
By default a VDI host is enabled in the farm. When it is disabled, published applications and virtual desktops cannot be served from it.

To disable a server from the farm untick the option **Enable Server in farm** from the **Properties** tab in the Server Properties. Tick back (enable) any of the tick boxes to enable the server back in the farm.

Configuring VDI Host Connection Settings

From the **Properties** tab in the **Server Properties** you can configure any of the below settings:

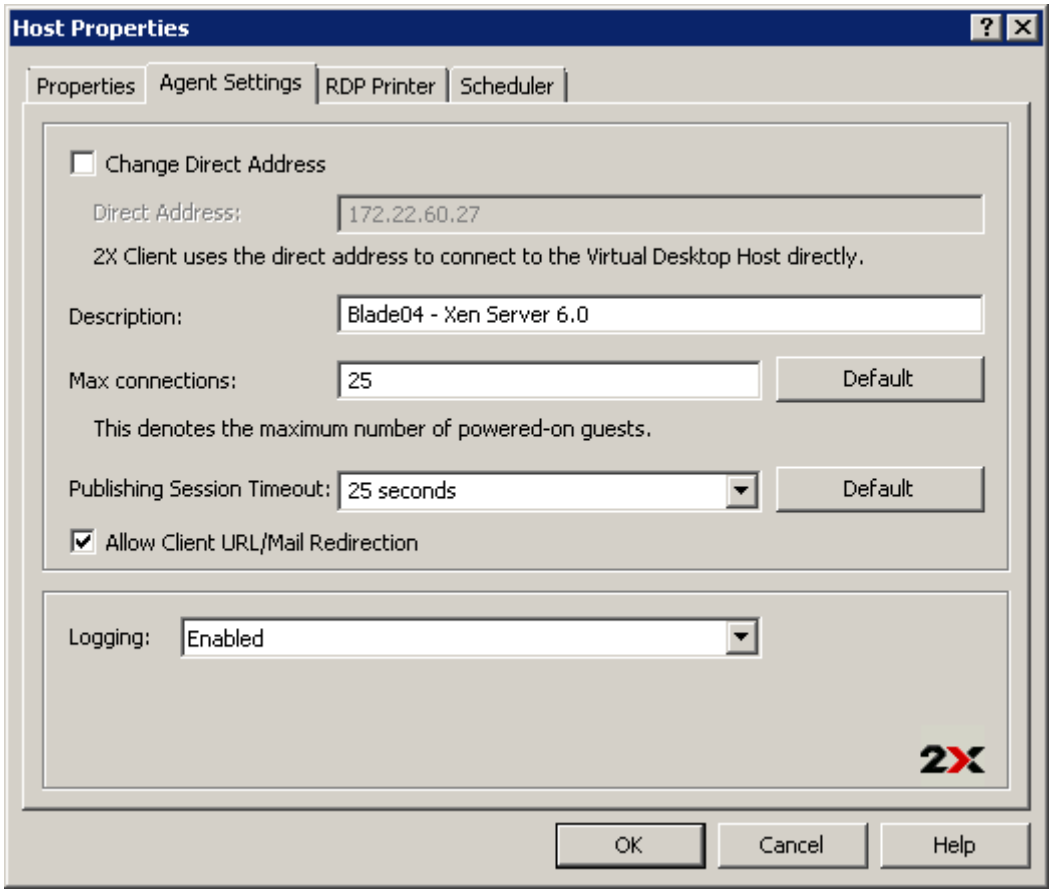
- **VDI Type**
- **VDI Version**
- **VDI Host** IP Address or FQDN
- **VDI Port**
- **VDI Agent IP Address** (if the agent is running on an appliance)
- **Username** and **Password** in case server requires different credentials



Configuring the Properties and connection settings of a VDI Host

Configuring the 2X VDI Agent on the Server

Each VDI Host server in the farm has a 2X Agent installed (or running as an appliance) to provide a connection between the 2X ApplicationServer XG and the VDI Host. The agent can be configured from the **Agent Settings** tab in the server properties.



Configuring VDI Agent from the Agent Settings Tab in the VDI Host Properties

Changing the Direct Address

This address is only used in Direct Connection mode and it could be an internal or external IP. To change the Direct Address of a remote PC tick the option **Change Direct Address** and specify the new address in the **Direct Address** input field.

Changing the Maximum Number of Connections to the VDI Host

You can change the maximum number of connections that can connect to the VDI host from the **Max Connections** input field. Click the **Default** button to reset the value to the default configured value.

Change the Session Timeout

To change the amount of time each session remains connected in the background after the user has closed the published application specify a new value in the **Publishing Session Timeout** input field. This option is used to avoid unnecessary reconnections with the guests.

Configuring URL and Mail Redirect / Restricting Access

To allow http and mailto links to be opened using a local application on the client computer rather than the server's resources, enable the option **Allow Client URL/Mail Redirection**.

Configuring 2X VDI Agent Logging

To enable or disable the 2X VDI Agent logging use the **Logging** drop down menu. Such logging should only be enabled if instructed by the 2X support team.

Configuring RDP Printing for VDI Host

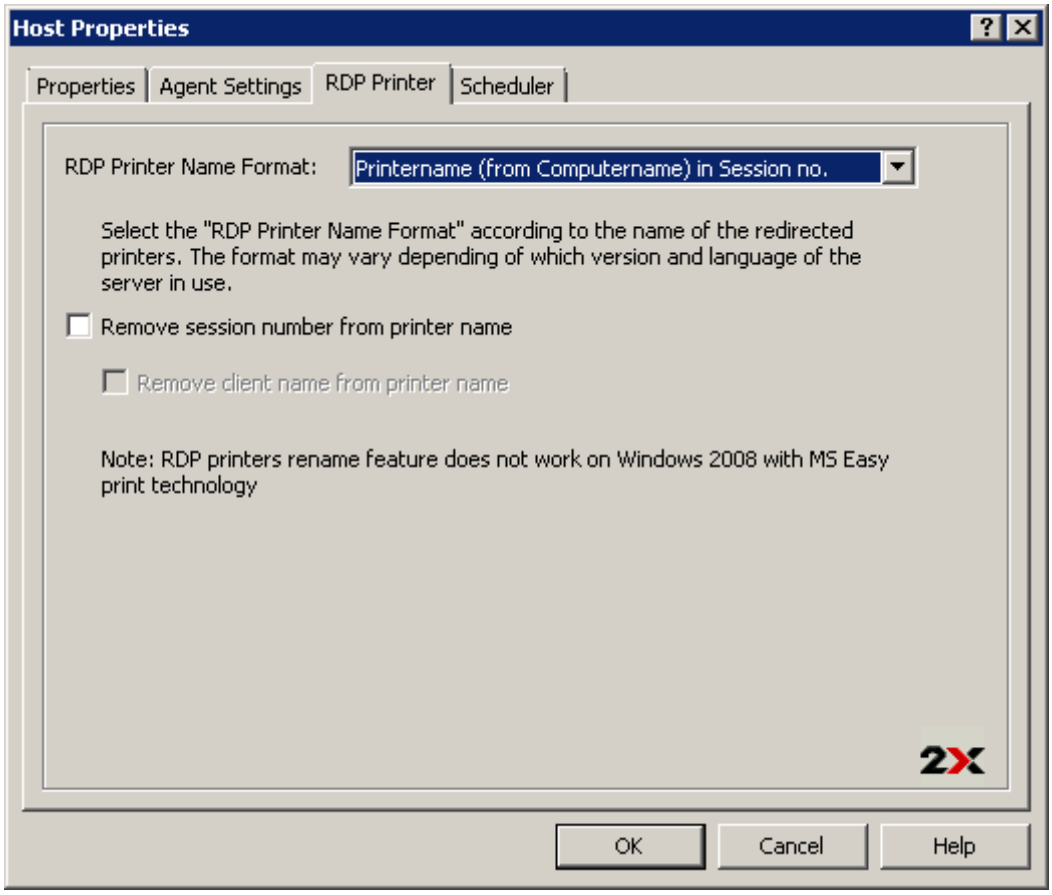
The **RDP Printer** tab allows you to configure the renaming format of redirected printers. The format may vary depending of which version and language of the server you are using. Set

your RDP Printer Name Format specifically for the configured server by choosing any of the below options from the **RDP Printer Name Format** drop down menu:

- Printername (from Computername) in Session no.
- Session no. (computername from) Printername
- Printername (redirected Session no)

The other RDP Printing options available in the RDP Printer tab are:

- Remove session number from printer name
- Remove client name from printer name


Host Properties
Properties
Agent Settings
RDP Printer
Scheduler
RDP Printer Name Format:
Printername (from Computername) in Session no.
Select the "RDP Printer Name Format" according to the name of the redirected printers. The format may vary depending of which version and language of the server in use.
Remove session number from printer name
Remove client name from printer name
Note: RDP printers rename feature does not work on Windows 2008 with MS Easy print technology
2X
OK
Cancel
Help

Configuring RDP Printers for a VDI Host

Configuring VDI Host Maintenance Time Window

From the **Scheduler** tab in the VDI host properties you can create and configure a maintenance time window for the server. During a maintenance window published resources won't be accessible from that server. To configure a maintenance time window click the **Add** button to configure the:

- Start date
- Time
- Duration
- Repeat: from this option configure the repeat interval of the maintenance time window, for example every week, month etc.

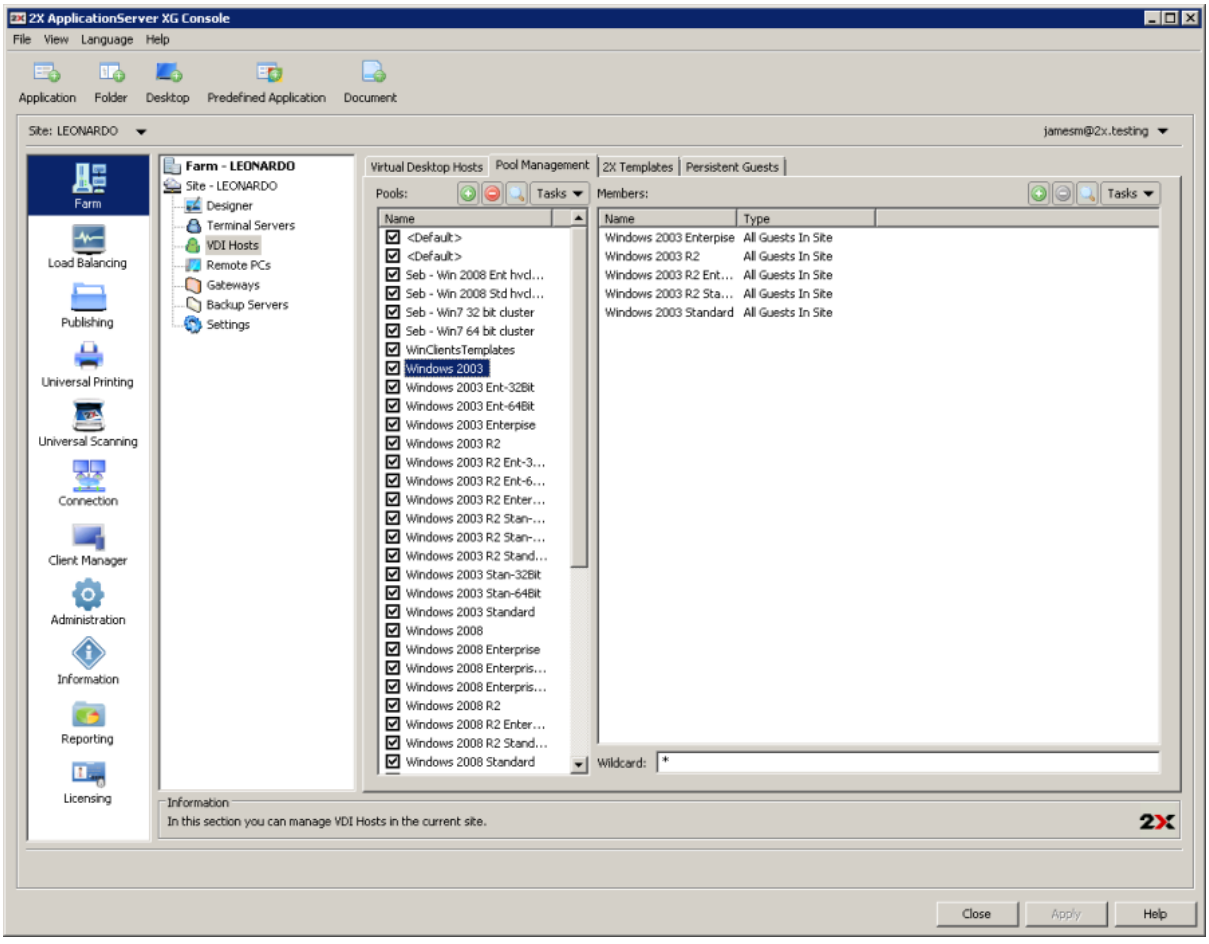
Once you configure the time for the maintenance window, use the drop down menu **On Disable** to specify what happens of the current sessions once the server has been disabled for maintenance.

Configuring and Managing Pools

Introduction

Pools offer administrators more flexibility when managing an extensive number of Guests, especially when they are implemented in large company infrastructures. The 2X ApplicationServer Console provides the framework and tools needed to create a complete Pool Management foundation.

Pools can be managed from the **Pools Management** tab in **VDI Hosts** node from the 2X ApplicationServer Console, as seen in the screenshot below.



Managing Pools for VDI Hosts

Adding and Deleting Pools

Adding a Pool

To add a Pool click **Add** from the **Tasks** drop down in the **Pools** column and specify a name.

Deleting a Pool

To delete a Pool highlight the Pool name and select **Delete** from the **Tasks** drop down menu in the **Pools** column.

Managing Members in a Pool

Adding Members to a Pool

To add members to a pool, navigate to the **Pools Management** tab, highlight the Pool's name and click **Add**. You can add any of the following:

- **All Guests in Site**: All guests on all VDI hosts that are located in the site.
- **All Guests in Host**: All guests that are located on a particular VDI host.
- **Guest**: A single guest located in the farm.
- **Native Pool**: Group of guests that have been previously configured from the hypervisor management tool as a pool. **Note:** hypervisor may use different terminology instead of pools (e.g. resource pools)
- **Pool**: Add an already existing configured pool in the 2X ApplicationServer XG (pool nesting)
- **2X Template**: Guests that are automatically created from a 2X Template. For more information about 2X Templates refer to the section Configuring and Managing 2X Templates for Guest Clones on page 44.

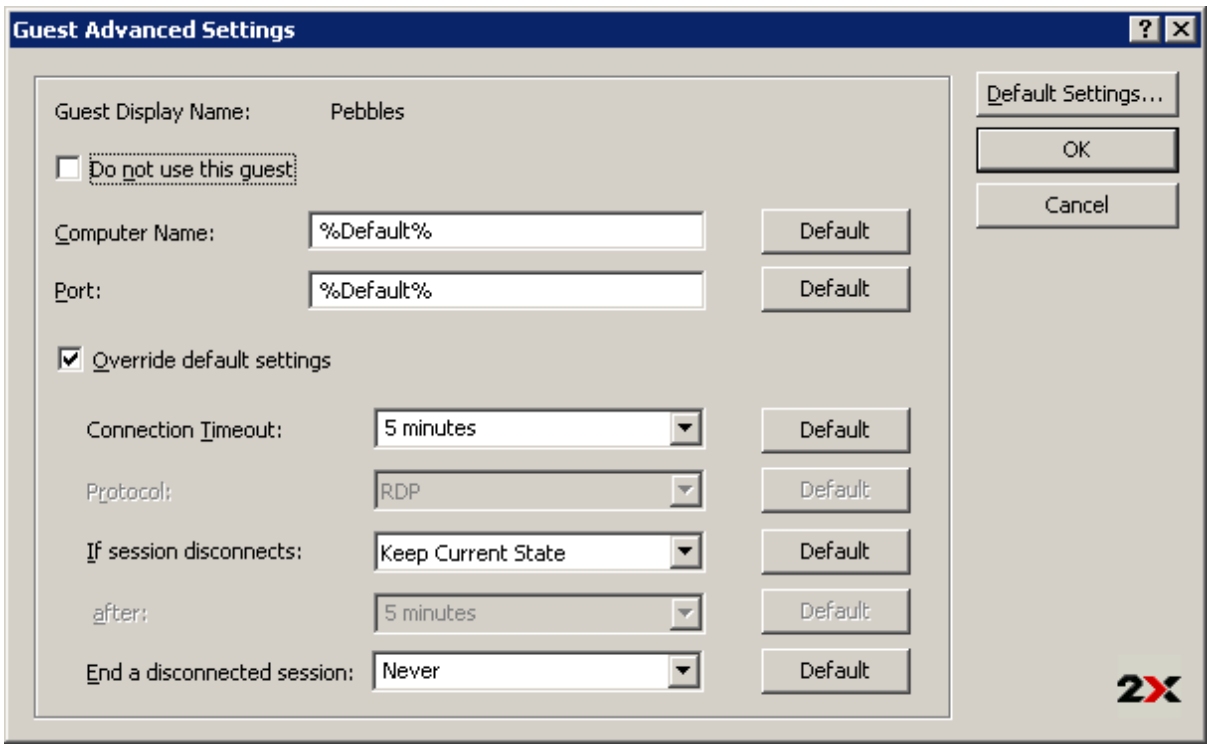
Once you select the type of member to add to a Pool you will be presented with the list of available pools or guests. Highlight the name of the member you would like to Add to the Pool and click **OK**.

Deleting a Member from a Pool

To delete a member from a Pool, highlight the Pool name, click on the pool member and click **Delete** from the **Tasks** drop down menu.

Configuring Virtual Guests in a Pool

You can configure all virtual guests in a VDI host or in a Pool. To configure a virtual guest from a Pool highlight the Pool name and from the **Tasks** drop down menu of the **Pools** column select **Show Guests in a** Pool. Once in the **Virtual Guest List** dialog box highlight the virtual guest name and click **Properties**.



From the **Guest Advanced Settings** dialog box shown in the screenshot above you can configure the following settings:

- Enable **Do not use this guest** checkbox so the system ignores the particular Virtual Guest.
- Specify a computer name in the **Computer Name** field to set the network name (domain name / IP address) of the computer that the system will use to connect to the Virtual Guest.
- Specify a port number in the **Port** field that the system will use to connect to the Virtual Guest.
- In the **Connection Timeout** field set a time limit the 2X ApplicationServer XG has to wait when connecting until the connection times out.
- Select the protocol from the **Protocol** drop down menu the 2X ApplicationServer XG uses to communicate with the Virtual Guest.
- Specify what happens of the Virtual Guest if a user disconnects from a session by choosing an option from the **If session disconnects** drop down menu. You can also specify the amount of time that needs to pass before the selected action is taken from the **After** input field.
- You can also specify to end a disconnected or not from the **End a disconnected session** drop down menu. From the same drop down menu you can also specify the amount of time that needs to pass before a disconnected session is terminated. **Note:** The user can reconnect to a previous session if the session is still available.

Configuring Virtual Guests Default Settings

In the **Virtual Guests List** dialog box click the **Default Settings** button to specify the default settings for all the virtual guests in the pool.

Resetting Virtual Guest Settings to Default

To reset the virtual guest's settings to the default settings highlight the virtual guest name from the **Virtual Guests List** dialog box and click the **Clear Settings** button.

Using the Wildcard Function

Use the **Wildcard** input field at the bottom of the **Pool Management** tab to match specific guests for the available guests within the pool which will be available for the user. Therefore if some of the virtual guests names won't match the wildcard, they won't be available for the users.

For example, XP* will match only guests whose name starts with XP and *XP* will match guests which have XP in any part of their name.

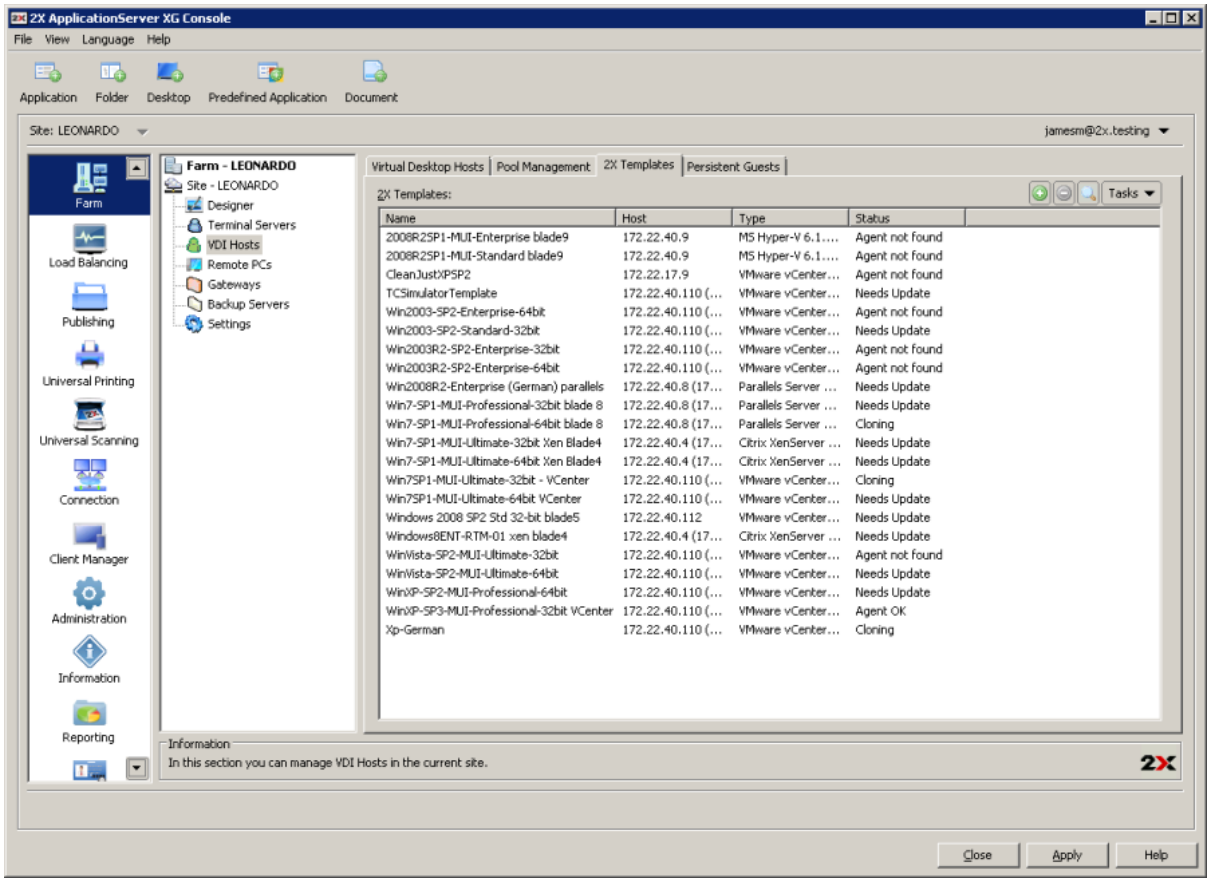
Configuring and Managing 2X Templates for Guest Clones

Introduction

2X Templates allow you to better utilize host resources by automatically creating and deploying virtual guests clones when needed. 2X Templates and clones can only be created for the following Windows workstations:

- Windows XP SP3
- Windows Vista
- Windows 7

- Windows 8


2X ApplicationServer XG Console
File View Language Help
Application Folder Desktop Predefined Application Document
Site: LEONARDO
jamesm@2x.testing
Farm
Load Balancing
Publishing
Universal Printing
Universal Scanning
Connection
Client Manager
Administration
Information
Reporting
Farm - LEONARDO
Site - LEONARDO
Designer
Terminal Servers
VDI Hosts
Remote PCs
Gateways
Backup Servers
Settings
Virtual Desktop Hosts
Pool Management
2X Templates
Persistent Guests
2X Templates:
Tasks
Name
Host
Type
Status
2008R2SP1-MUI-Enterprise blade9 172.22.40.9 MS Hyper-V 6.1.... Agent not found
2008R2SP1-MUI-Standard blade9 172.22.40.9 MS Hyper-V 6.1.... Agent not found
CleanJustXPSP2 172.22.17.9 VMware vCenter... Agent not found
TCSimulatorTemplate 172.22.40.110 (... VMware vCenter... Needs Update
Win2003-SP2-Enterprise-64bit 172.22.40.110 (... VMware vCenter... Agent not found
Win2003-SP2-Standard-32bit 172.22.40.110 (... VMware vCenter... Needs Update
Win2003R2-SP2-Enterprise-32bit 172.22.40.110 (... VMware vCenter... Agent not found
Win2003R2-SP2-Enterprise-64bit 172.22.40.110 (... VMware vCenter... Agent not found
Win2008R2-Enterprise (German) parallels 172.22.40.8 (17... Parallels Server ... Needs Update
Win7-SP1-MUI-Professional-32bit blade 8 172.22.40.8 (17... Parallels Server ... Needs Update
Win7-SP1-MUI-Professional-64bit blade 8 172.22.40.8 (17... Parallels Server ... Cloning
Win7-SP1-MUI-Ultimate-32bit Xen Blade4 172.22.40.4 (17... Citrix XenServer ... Needs Update
Win7-SP1-MUI-Ultimate-64bit Xen Blade4 172.22.40.4 (17... Citrix XenServer ... Needs Update
Win7SP1-MUI-Ultimate-32bit - VCenter 172.22.40.110 (... VMware vCenter... Cloning
Win7SP1-MUI-Ultimate-64bit VCenter 172.22.40.110 (... VMware vCenter... Needs Update
Windows 2008 SP2 Std 32-bit blade5 172.22.40.112 VMware vCenter... Needs Update
Windows8ENT-RTM-01 xen blade4 172.22.40.4 (17... Citrix XenServer ... Needs Update
WinVista-SP2-MUI-Ultimate-32bit 172.22.40.110 (... VMware vCenter... Agent not found
WinVista-SP2-MUI-Ultimate-64bit 172.22.40.110 (... VMware vCenter... Needs Update
WinXP-SP2-MUI-Professional-64bit 172.22.40.110 (... VMware vCenter... Needs Update
WinXP-SP3-MUI-Professional-32bit VCenter 172.22.40.110 (... VMware vCenter... Agent OK
Xp-German 172.22.40.110 (... VMware vCenter... Cloning
Information
In this section you can manage VDI Hosts in the current site.
2X
Close
Apply
Help

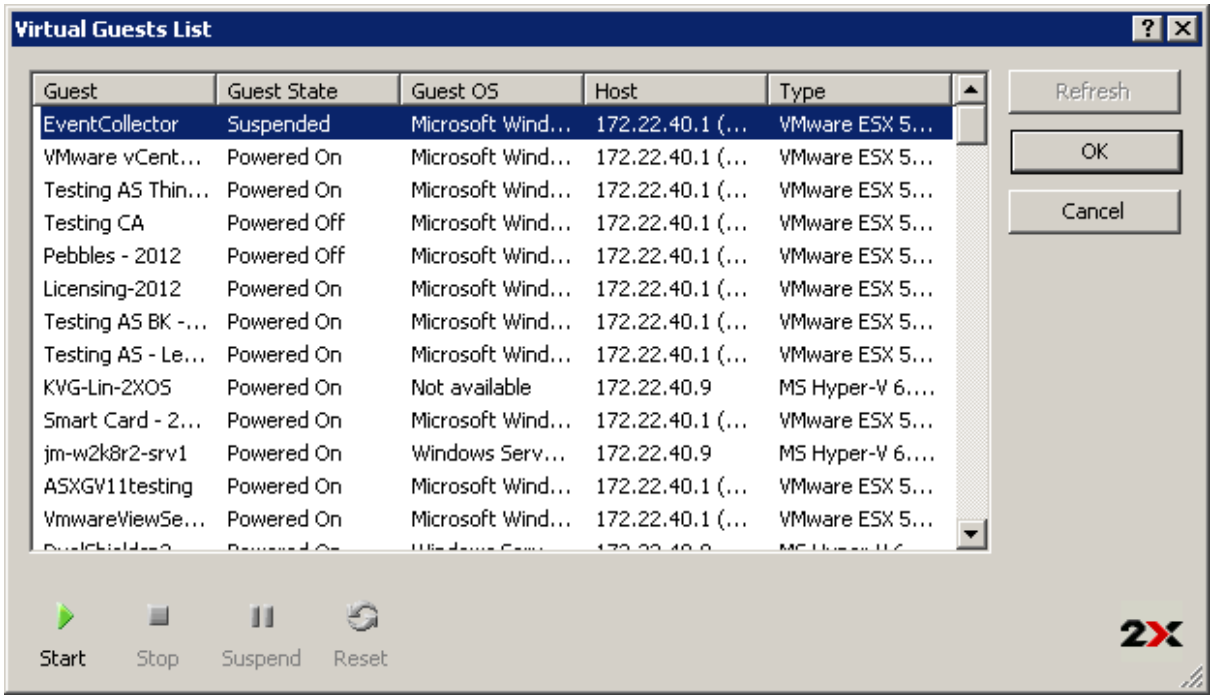
Managing 2X Templates from the 2X Templates Tab

Creating a 2X Template

Requirement: To create a template of a Windows workstation the machine should be configured to obtain an IP via a DHCP server.

To create a new 2X Template of a Windows workstation follow the below procedure:

1. Navigate to the **Farm** category, click the **2X Templates** tab from the **VDI Hosts** node and click **Add** from the **Tasks** drop down menu.
2. Select a guest from which you would like to create a 2X template from the **Virtual Guests List** dialog box, shown in the screenshot below and click **OK**.



List of available guests to create a 2X Template from

3. In the next step of the process the 2X ApplicationServer XG will check if the virtual guest has the 2X Guest Agent installed. If it is not installed click the **Install** button.
4. In the **Installing 2X Guest Agent** dialog box you can specify different credentials to connect to the server by clicking the option **Override system credentials** and specifying new credentials. Click **Install** to proceed with the agent installation and click **Done** once it has been successfully installed. (If the automatic installation of the 2X Agent fails, refer to the Section Installing the 2X Terminal Server Agent Manually on page 23.
5. Once the 2X Guest Agent is installed click **OK**.

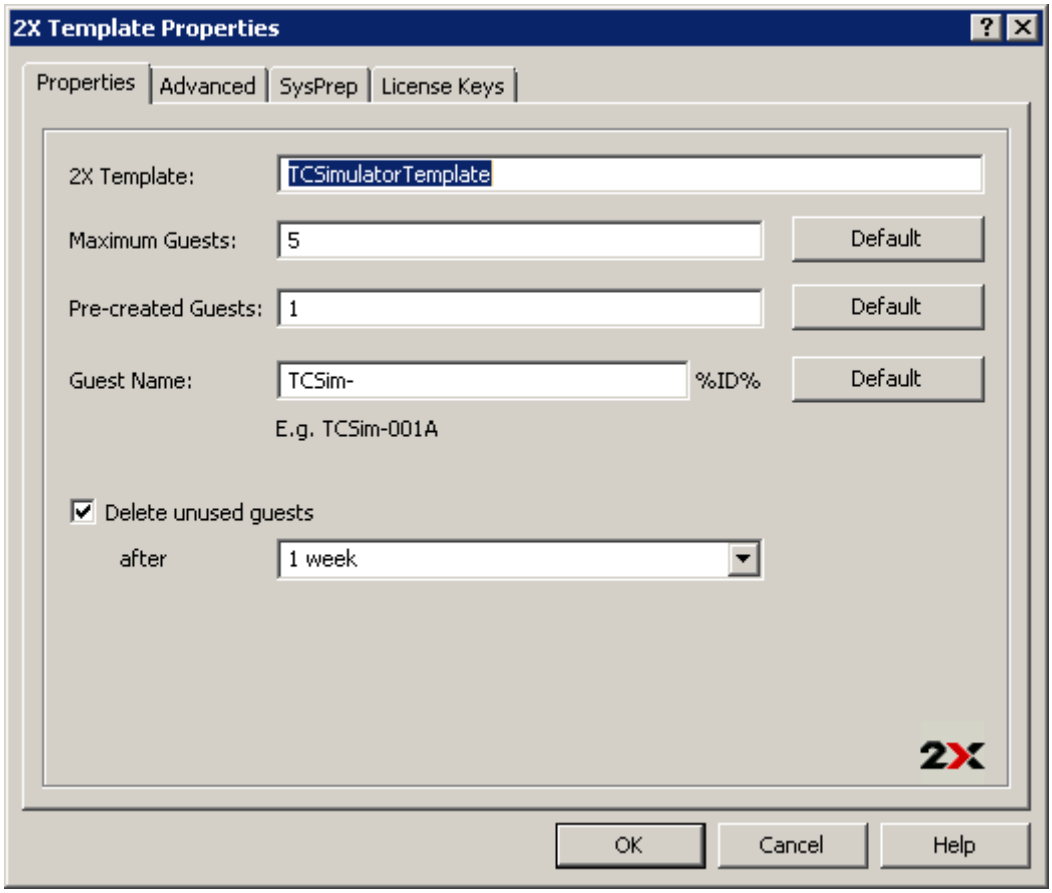
Configuring a 2X Template

To configure a 2X Template highlight the template name from the **2X Templates** node and click **Properties** from the **Tasks** drop down menu.

Basic 2X Template Settings – Configuring Maximum Guests and Pre-Created Guests

From the **Properties** tab shown in the below screenshot you can configure any of the following settings:

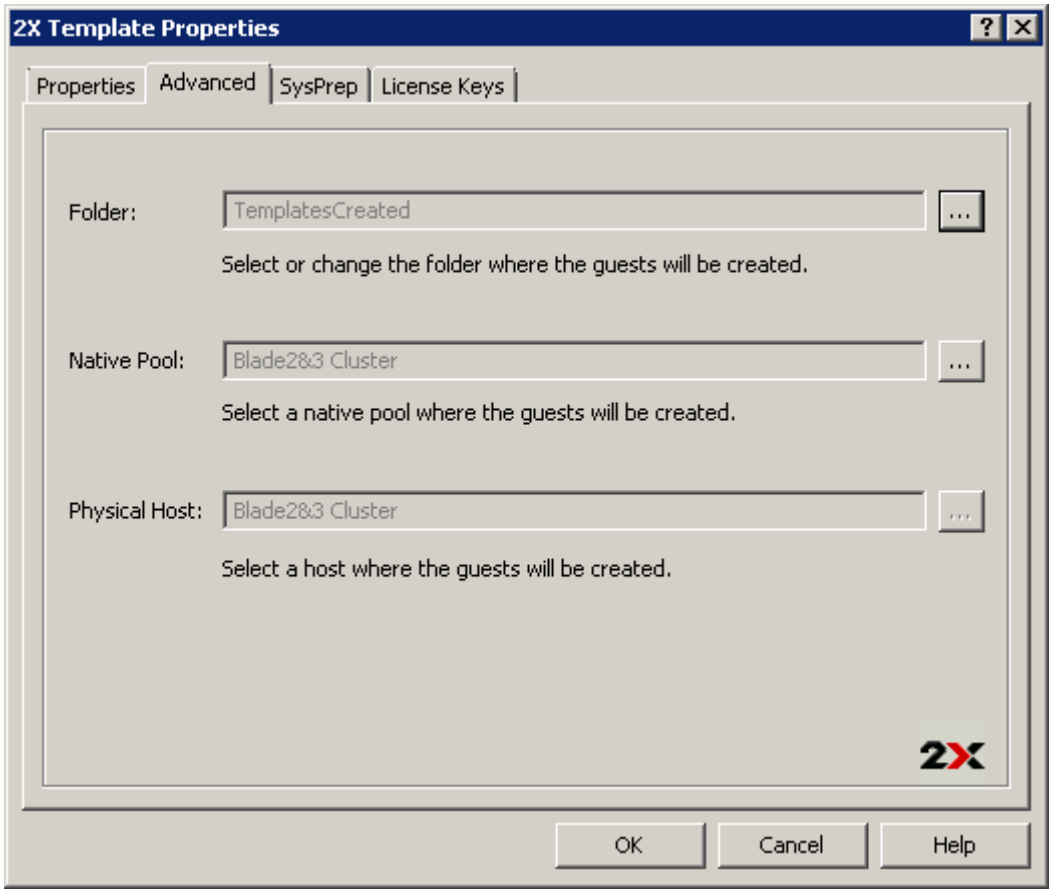
- **2X Template**: Name for the template
- **Maximum Guests**: Specify the maximum number of guest clones that can be created
- **Pre-created Guests**: Specify the number of guest clones that will be pre-created so they are always available for users to connect to.
- **Guest Name**: Specify the guest clones machine name. Note that each guest clone name will be appended with the Guest ID.
- **Delete unused guests**: Enable this option to delete all guest clones that are not being used. You can also specify the time for a guest clone to be considered as unused from the **after** drop down menu.



2X Templates Properties

Configure Location Where Virtual Guest Clones will be Stored

From the **Advanced** tab you can configure the folder where newly created guest clones created from the 2X Template will be created in the **Folder** input field. This option is available if you are using Hyper-V, Parallels Server4, Citrix Xen and VCenter.



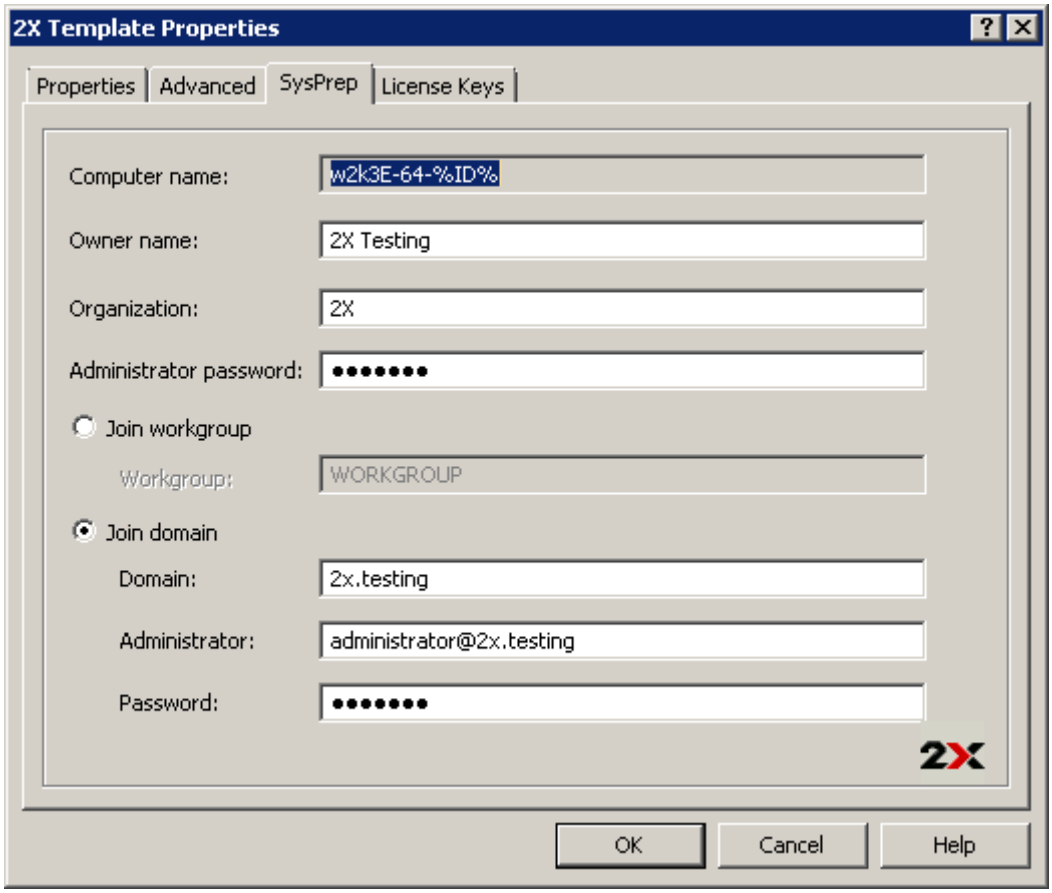
Configuring the location where Virtual Guest Clones will be stored

If the hypervisor you are using supports Native Pools, the newly created guest clones will be part of the specified **Native Pool** location. This option is available if you are using VMWare ESX, VMWare VCenter and VMWare Server 2.

Configuring SysPrep for Virtual Guest Clones

From the **SysPrep** tab shown in the below screenshot you can configure SysPrep settings for the virtual guest clones in the 2X Template. The following options can be configured:

- **Computer Name**
- **Owner Name**
- **Organization**
- **Administrative Password**
- **Join Workgroup**: select this option and specify a workgroup if the virtual guest clone will be part of a workgroup
- **Join domain**: select this option and specify a domain and credentials to join the domain if the virtual guest clone will be part of a domain.



Configuring sysprep settings for virtual guest clones

Configuring License Key and Limit for Virtual Guest Clone

From the **License** tab you can specify the operating system license key and the key limit.

Updating the Template Operating System

If you need to update the template operating system, such as installing a service pack or new software, you need to put the template into maintenance mode. To put a template into maintenance mode highlight the template name from the template list and click **Maintenance** from the **Tasks** drop down menu.

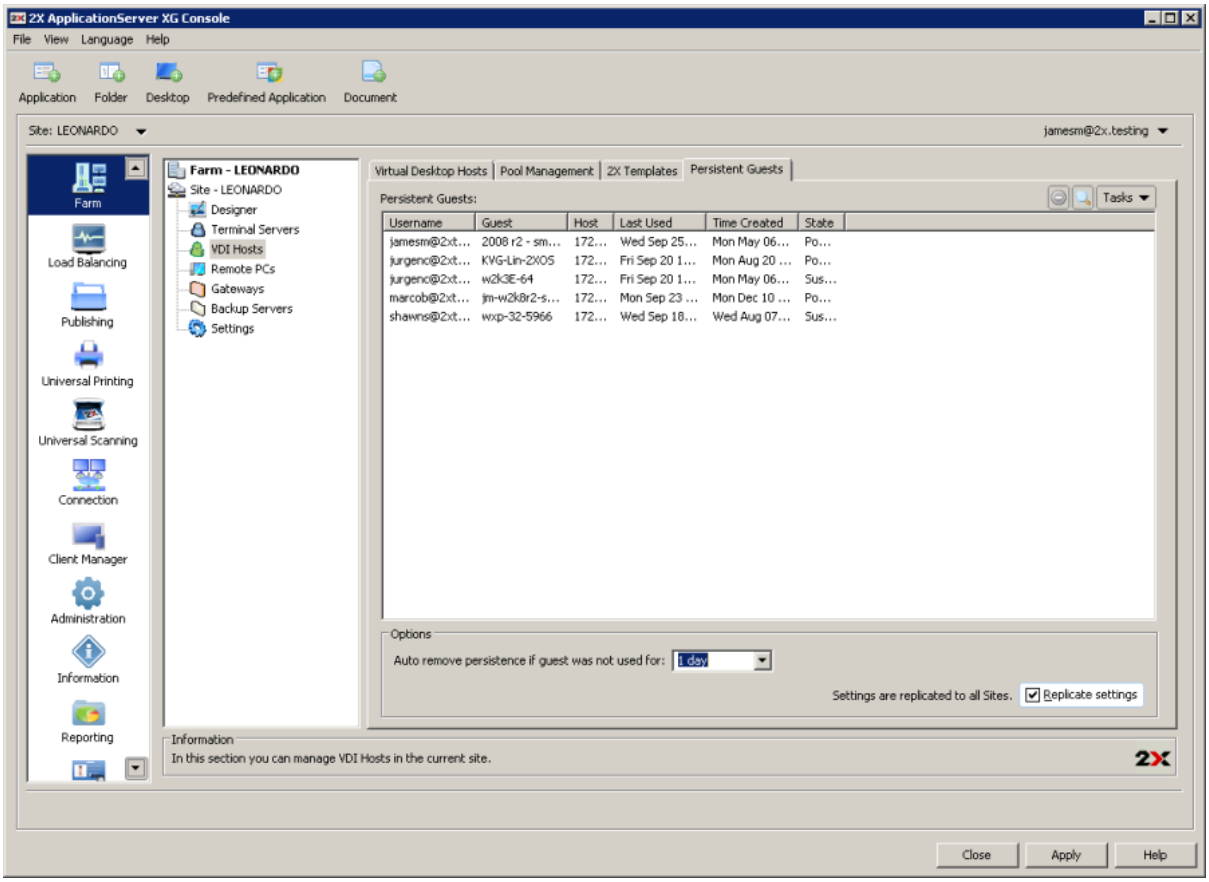
Note: While in maintenance mode, clones cannot be created from the guest and the entry in the list of 2X templates will be greyed out.

During the maintenance mode, the template OS is booted and can be modified. Once the changes have been applied you can put the template off Maintenance Mode by clicking again the **Maintenance** button.

Note: Updates applied to the template OS during maintenance mode will only affect newly created clones. Already created clones will not be affected.

Persistent Guests

When a published application or desktop from a virtual guest is set as persistent, the first time a user launches the application or desktop the publishing agent will create a persistent guest rule. Persistent Guests rules can be accessed from the **Persistent Guests** tab seen in the below screenshot.



Configuring persistent guests from the Persistent Guests tab

Deleting a Persistent Guest Rule

To delete a persistent guest rule highlight the rule from the **Persistent Guests** tab and click **Delete** from the **Tasks** drop down menu. If you want to delete all rules, select all rules by pressing CTRL+A and hit the delete key.

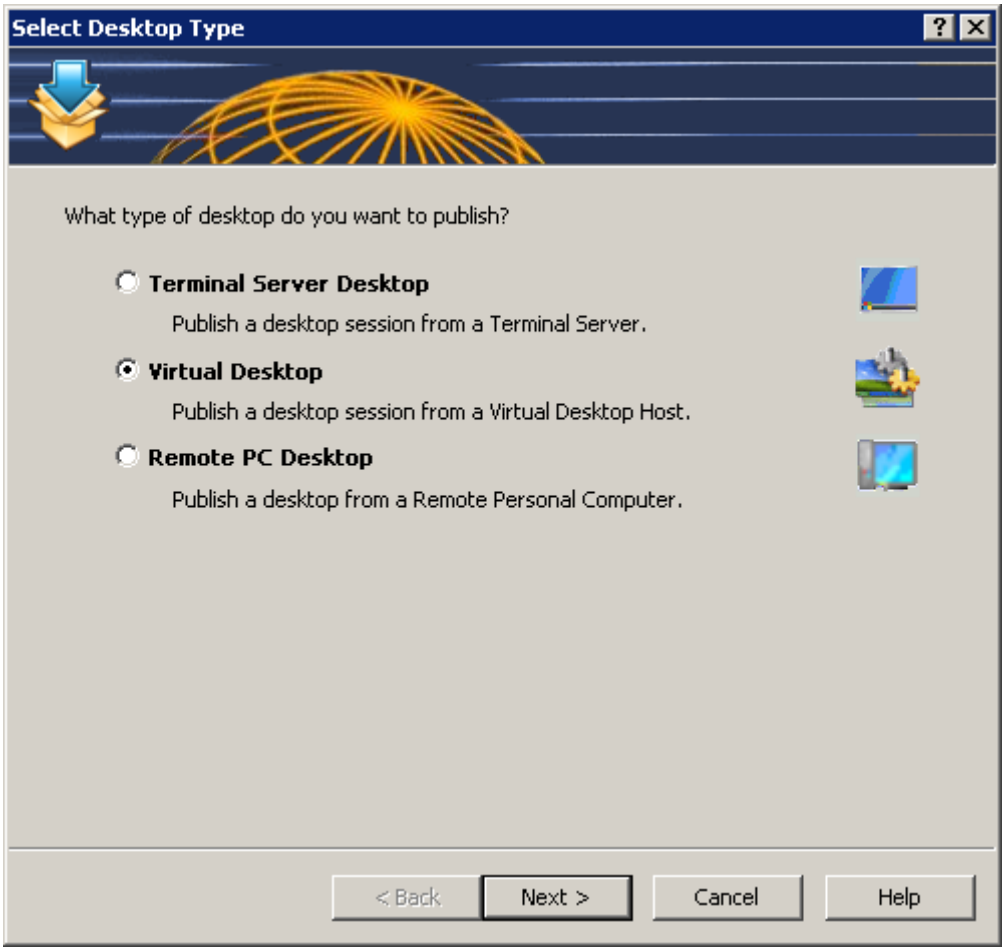
Configuring Automatic Deleting of Persistent Guest Rules

From the **Auto remove persistence if guest was not used for** drop down menu at the bottom of the **Persistent Guests** tab you can specify the maximum time an unused persistent guest rule is kept before being automatically deleted. Alternatively you can also manually type in the desired time, for example 1 week 3 days.

Publishing a Virtual Desktop from a Guest

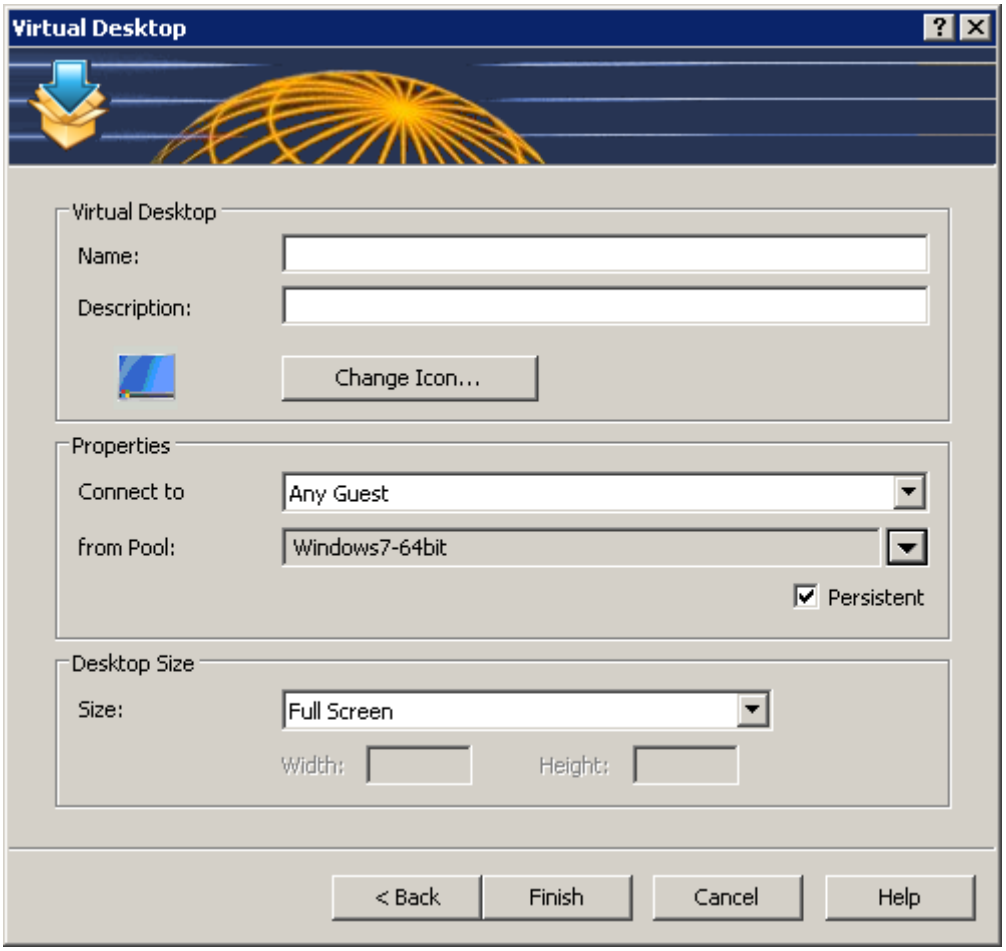
To publish a virtual desktop from a guest or guest clone follow the below procedure:

1. Click the **Publishing** category and click the **Desktop** icon from the top navigation bar.
2. Select **Virtual Desktop** in the first step of the wizard and click **Next**.


Select Desktop Type
What type of desktop do you want to publish?
Terminal Server Desktop
Publish a desktop session from a Terminal Server.
Virtual Desktop
Publish a desktop session from a Virtual Desktop Host.
Remote PC Desktop
Publish a desktop from a Remote Personal Computer.
< Back
Next >
Cancel
Help

Selecting Virtual Desktop from the Desktop Publishing Wizard

3. In the second step of the wizard enter a **Name** and **Description** in the **Virtual Desktop** section. From the same section you can also configure a different icon by clicking on the **Change Icon** button.
4. From the **Properties** section you have to specify from where the virtual desktop should be published. The options are:
    a. **Any Guest** from a specified pool in the **from pool** drop down menu
    b. **Specific guest**
    c. **Guest** from a specified pool in the **from pool** drop down menu where **name equals** username or IP
    d. **Specific 2X Template** from a specified 2X Template in the **2X Template** drop down menu
5. Tick the **Persistent** option to create a persistent guest rule the first time the user connections.
6. From the **Desktop Size** section you can specify the resolution of the desktop.



Configuring a Desktop to be Published

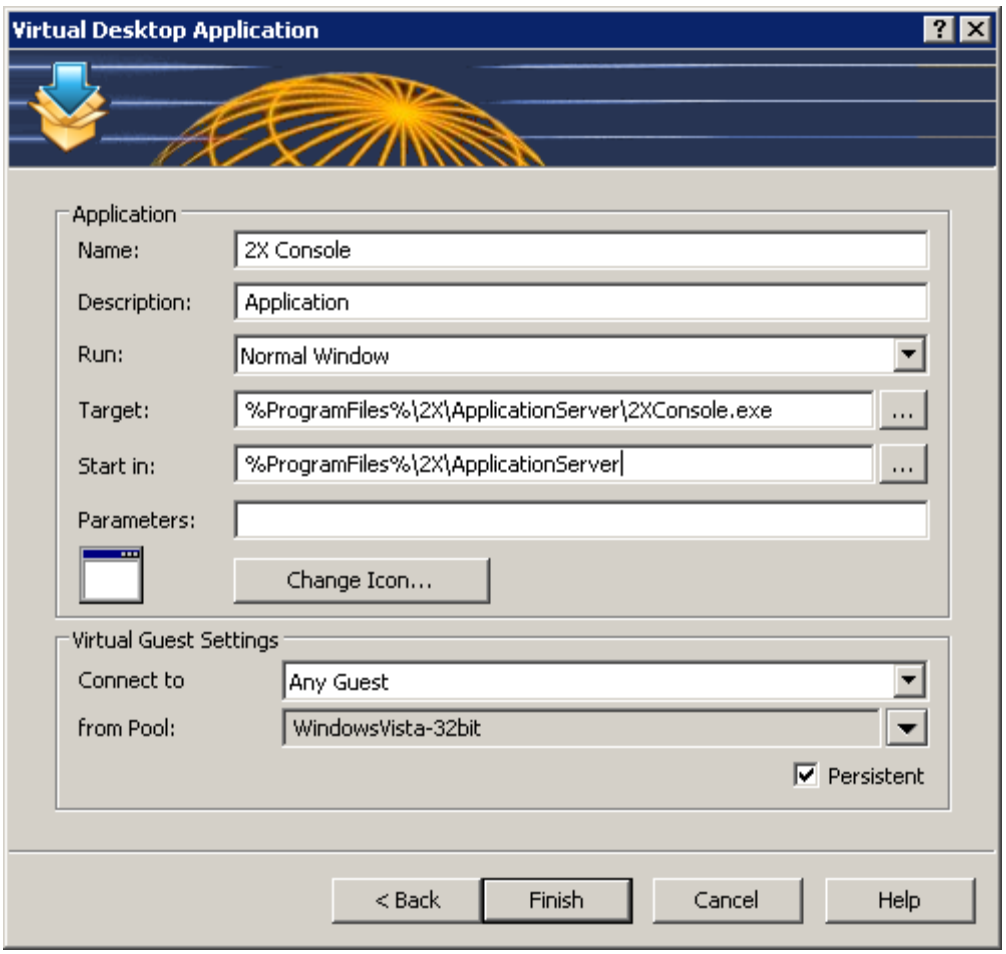
7. Once ready click **Finish** to publish the application.

Publishing an Application from a Guest

To publish an application from a guest or guest clone follow the below procedure:

1. Click the **Publishing** category and click the **Application** icon from the top navigation bar.
2. Select **Virtual Guest** in the first step of the wizard and click **Next**.
3. In the second step of the wizard select **Single Application** and click **Next**.
4. In the third step of the wizard browse to the application by clicking on the **Browse** button next to the **Target** input field so all details are populated. Alternatively you can configure all options manually by following the steps below.
5. Enter a **Name** and **Description** in the **Application section**.
6. From the **Run** drop down menu specify if the application should run in a normal window, maximized or minimized.
7. In the **Target** input field the path of where the application is installed should be specified. To specify a new path of the executable click the **Browse** (**...**) button and browse to the executable. Use Windows environment variables if you are manually entering the path.
8. In the **Start In** input field specify the folder that contains the original object or any other related file. For example sometimes applications need to use files from another location. In such cases specify such folder location so the published application will be able to locate them upon it being launched.
9. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application upon being started.

10. From the **Virtual Guest Settings** section you have to specify from where the application should be published. The options are:
    a. **Any Guest** from a specified pool in the **from pool** drop down menu
    b. **Specific guest**
    c. **Guest** from a specified pool in the **from pool** drop down menu where **name equals** username or IP
    d. **Specific 2X Template** from a specified 2X Template in the **2X Template** drop down menu
11. Tick the **Persistent** option to create a persistent guest rule the first time the user connections.



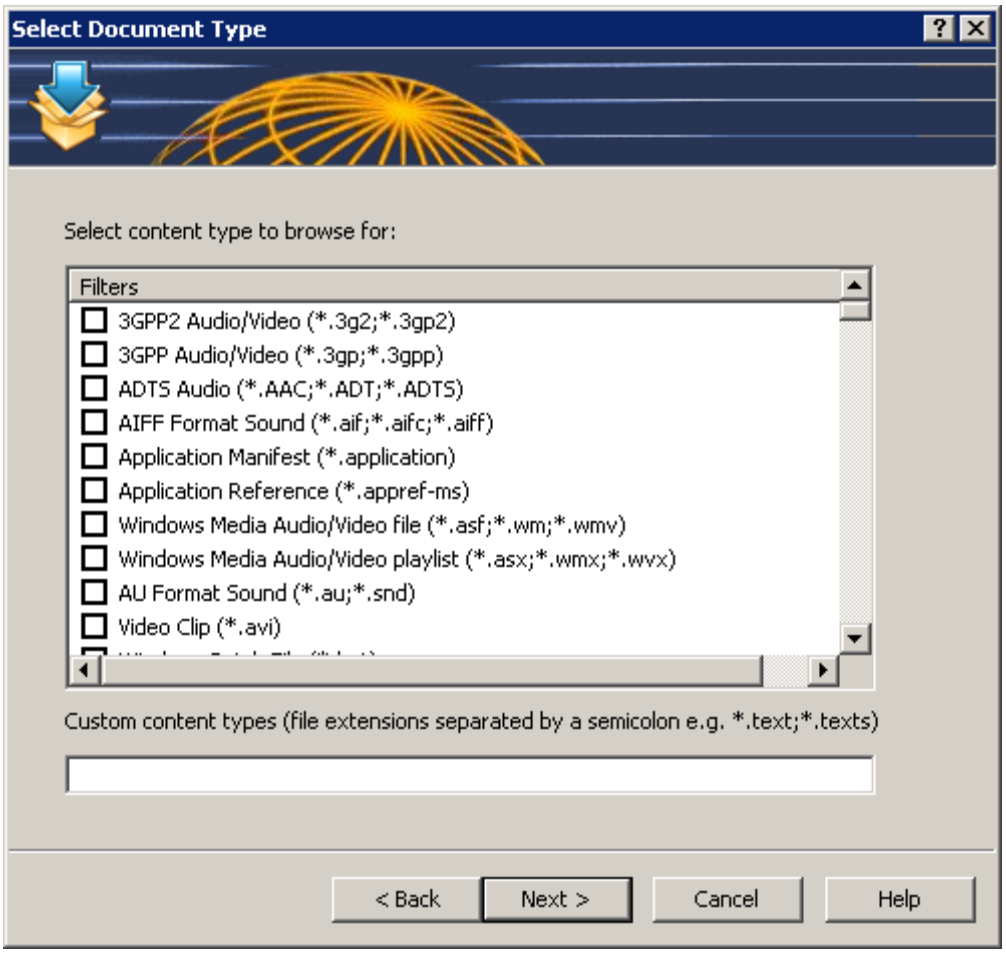
Configuring a Virtual Application to be Published

12. Once ready click **Finish** to publish the application.

Publishing a Document from a Guest

To publish a document from a guest or guest clone follow the below procedure:

1. Click **Publishing** from the system menu and click the **Document** icon from the top navigation bar.
2. Select **Virtual Guest** in the first step of the wizard and click **Next**.
3. In the second step specify the content type to browse for. You can also specify a custom content type from the **Custom content types** input field. Click **Next** once ready.

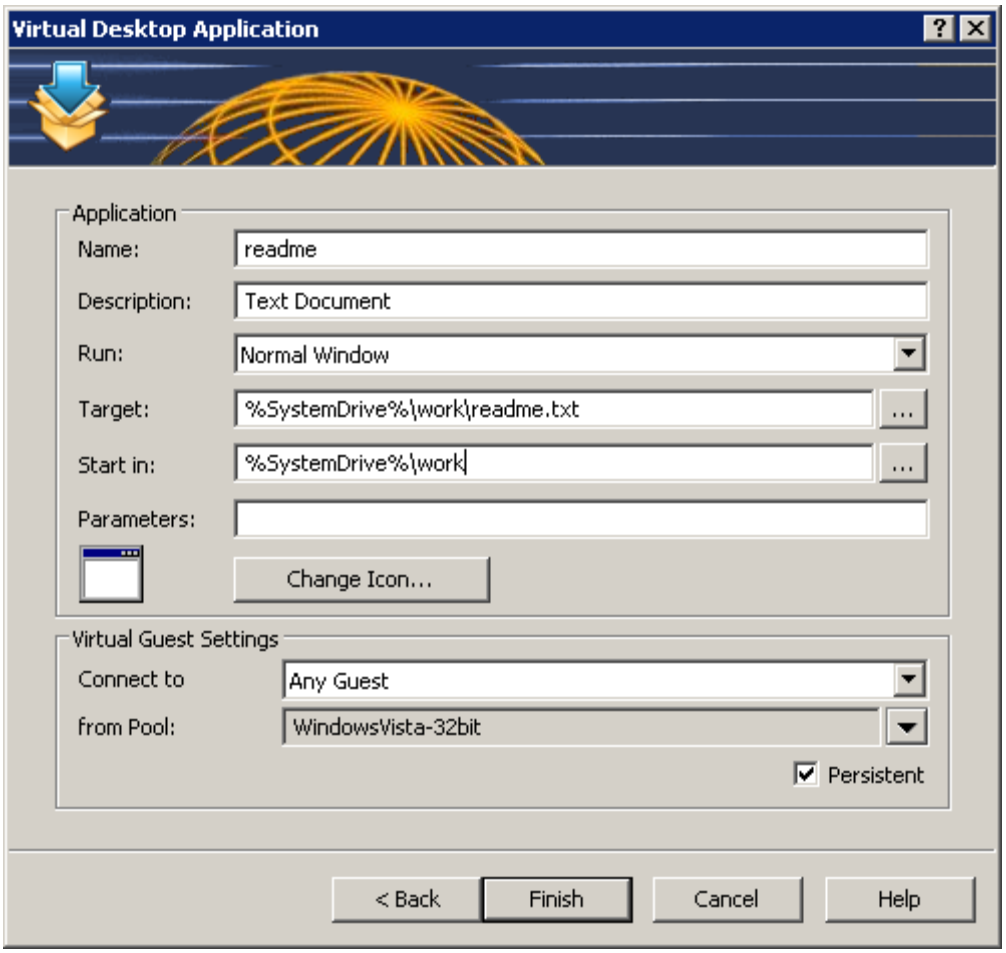


Configuring a Content Type for the Document

4. In the third step of the wizard use the **Browse** button next to the **Target** input field to browse to the document and all the other entries are automatically populated. If you would like to configure all entries manually follow the steps below.
5. Enter a **Name** and **Description** for the document in the **Application section**.
6. From the **Run** drop down menu specify if the application should run in a normal window, maximized or minimized.
7. In the **Target** input field the path of where the document is stored should be specified. To specify a new path of the executable click the **Browse** (**...**) button and browse to the document. Use Windows environment variables if you are manually entering the path.
8. In the **Start In** input field specify the folder that contains the original document or any other related file. For example sometimes applications need to use files from another location. In such cases specify such folder location so the published application will be able to locate them upon it being launched.
9. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application upon being started.
10. You can change the icon for the published application by clicking the **Change Icon** button and configure shortcut options by clicking the **Advanced Settings** button.
11. From the **Virtual Guest Settings** section you have to specify from where the application should be published. The options are:
    e. **Any Guest** from a specified pool in the **from pool** drop down menu
    f. **Specific guest**
    g. **Guest** from a specified pool in the **from pool** drop down menu where **name equals** username or IP

h. **Specific 2X Template** from a specified 2X Template in the **2X Template** drop down menu

12. Tick the **Persistent** option to create a persistent guest rule the first time the user connections.



Configuring a Virtual Document to be Published

13. Once ready click **Finish** to publish the application.

Remote PCs

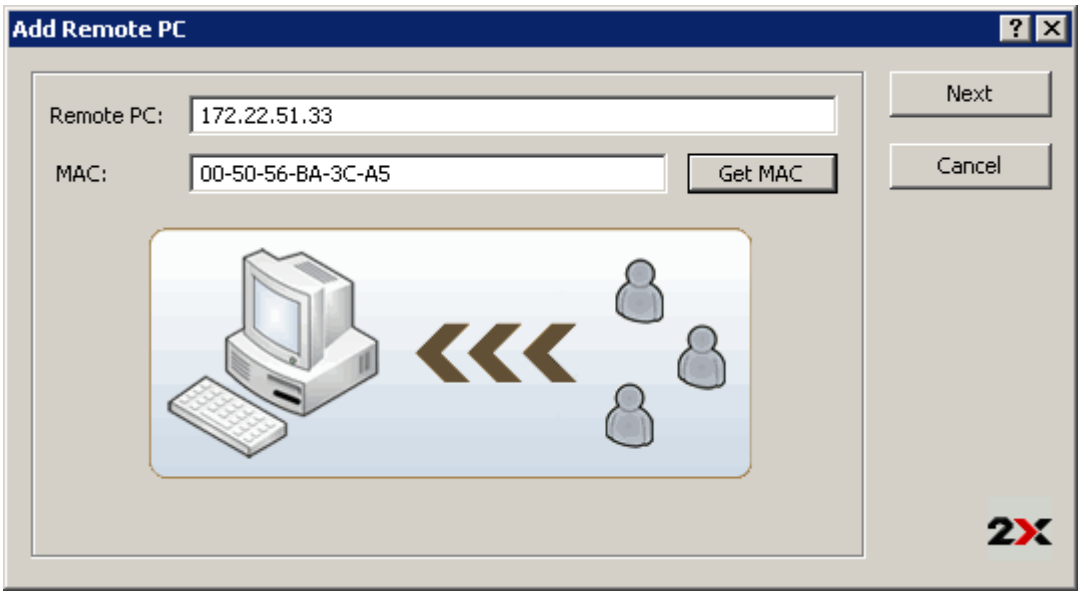
Introduction

Desktops and applications can also be published from any supported version of Microsoft Windows workstation operating system (Remote PCs). Remote PCs are similar to Guest Virtual Machines in the farm but typically they are standalone PC installations.

Adding a Remote PC

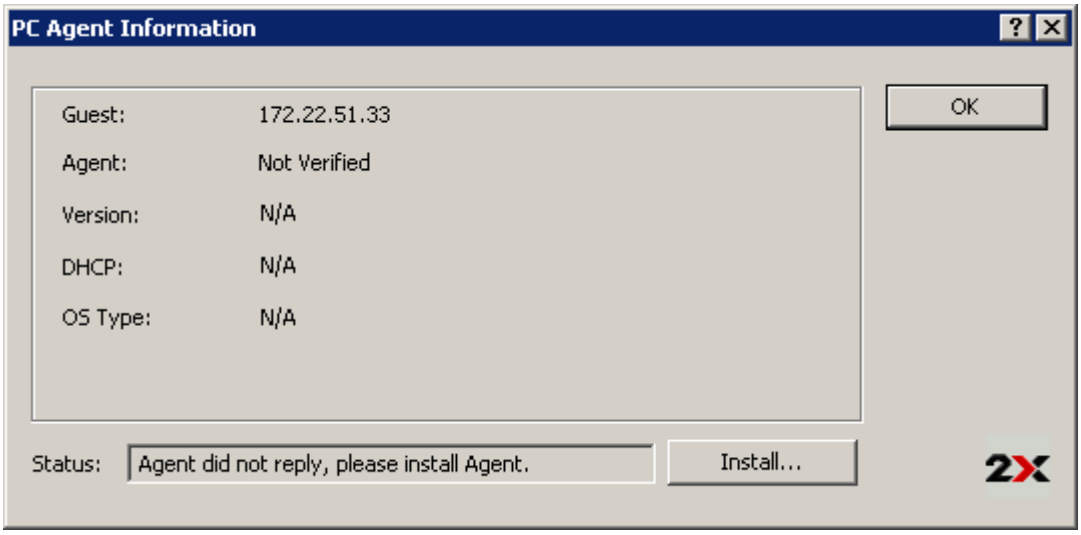
Follow the below procedure to add a Remote PC to the farm:

1. Launch the 2X ApplicationServer Console, select the **Farm** category and select on **Remote PCs** from the navigational tree.
2. Click **Add** from the **Tasks** drop down menu to launch the setup wizard and once prompted specify the server IP address or FQDN and click **Next**.



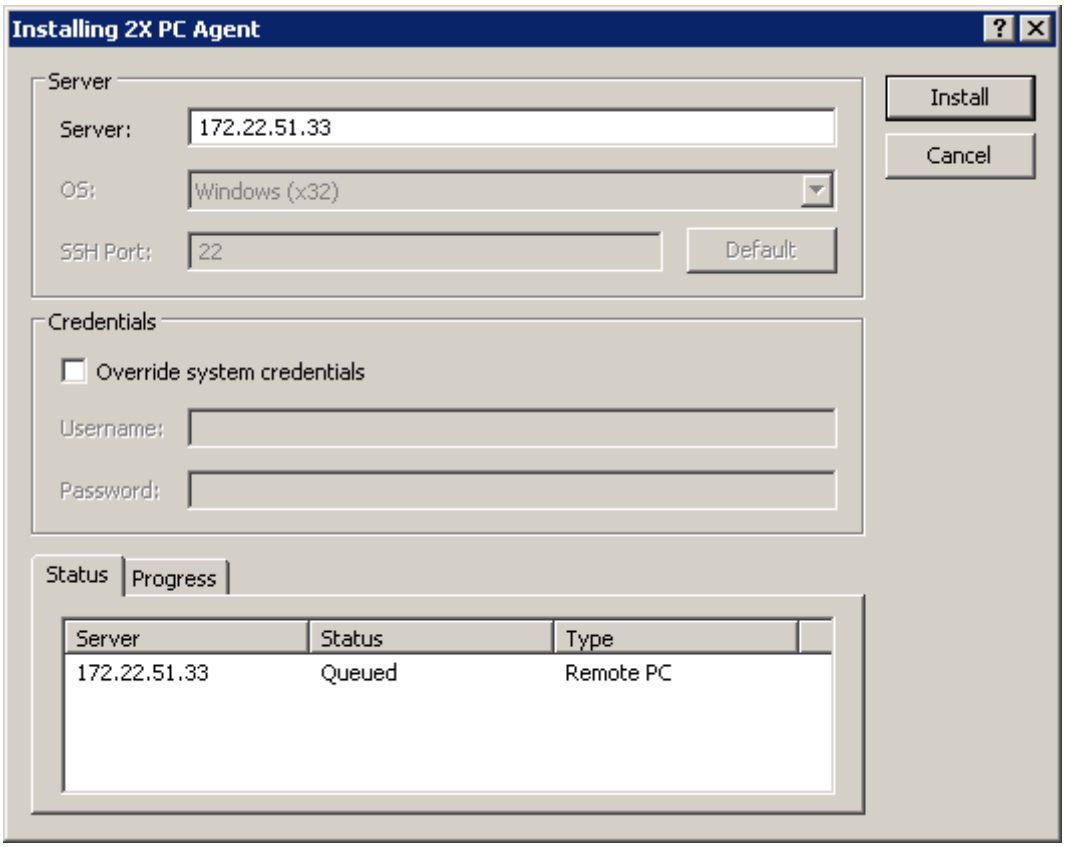
First Step of the Add a Remote PC Wizard

3. In this step the 2X ApplicationServer XG checks if the 2X agent is installed on the Remote PC. If it is installed, proceed to step 7 of this procedure. If it is not installed, click **Install** to remotely install the 2X agent.



2X ApplicationServer XG Checking if Remote PC Agent is Installed

4. In the **Installing 2X Remote PC Agent** dialog highlight the PC name on which the 2X Agent is to be installed.
5. (Optional) Tick the option “Override system credentials” to specify and use different credentials to connect to the PC and install the 2X Agent.
6. Click **Install** to install the agent and click **Done** once it has been successfully installed. If the automatic installation of the 2X Agent fails refer to the following section **Installing the 2X Remote PC Agent Manually**.



Installing 2X PC Agent Remotely

7. Click **Add** to add the Remote PC to the 2X ApplicationServer server farm.

Tip: Use the **Find** button to find existing terminal servers and citrix servers in your active directory domain.

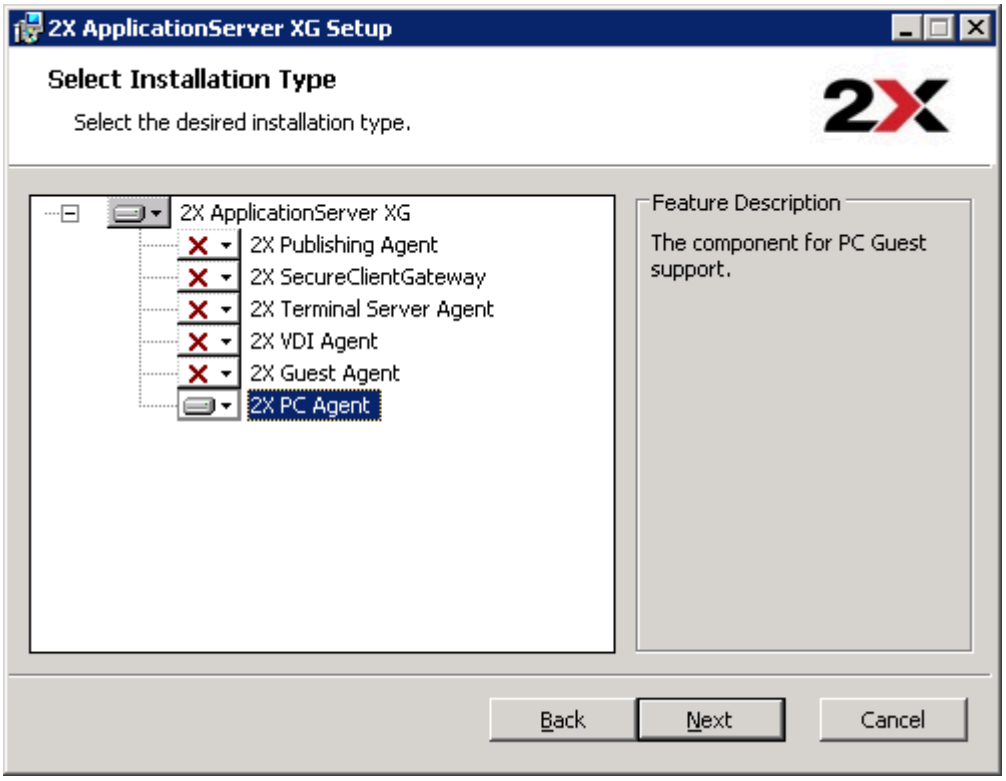
Installing the 2X Remote PC Agent Manually

2X Remote PC Agent System Requirements

- Windows XP, Windows Vista, Windows7.
- The same hardware requirements as specified by Microsoft when deploying a terminal services environment will apply.

Installing the 2X Remote PC Agent Manually

1. Login to the PC where the 2X Remote PC Agent is to be installed using an administrator account and close all other applications.
2. Copy the 2X ApplicationServer installation file (2XAppServer.msi) to the PC and double click it to launch the installation.
3. Once prompted click **Next** and accept the End-User license agreement.
4. Specify the path where the 2X Agent should be installed and click **Next**.
5. Select **Custom** and click **Next**.
6. Click on the 2X PC Agent and select **Entire Feature will be installed on local hard drive** from the drop down menu as seen in the below screenshot.



Manually Installing the Remote PC Agent

7. Ensure that all other components are deselected and click **Next**.
8. Click **Install** to start the installation and **Finish** once the installation is finished.

Note: The 2X Agent does not require any configuration. Once the 2X Agent is installed, highlight the Remote PC name in the 2X ApplicationServer Console and click **Check Agent**. If the agent is installed properly, the status should change to **Agent Installed** as seen in the below screenshot.

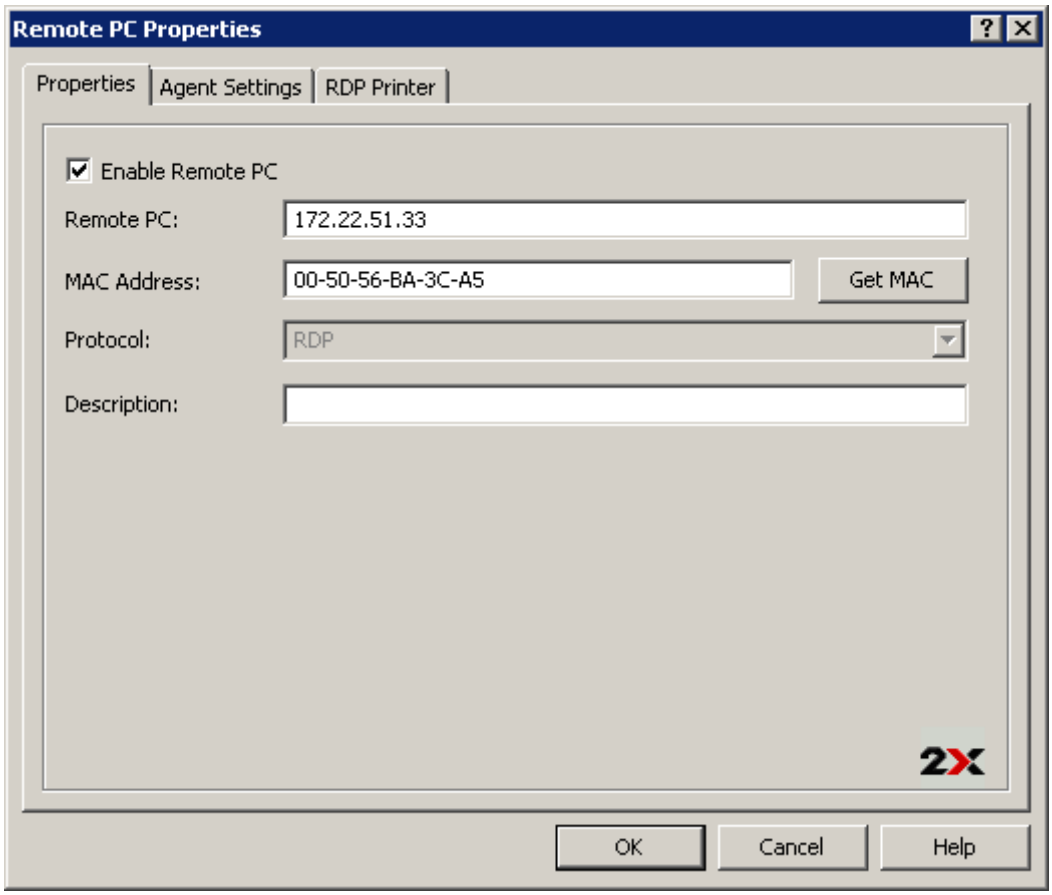
Configuring a Remote PC

To access the properties of a Remote PC highlight the computer name from the navigation tree in the 2X ApplicationServer Console and click **Properties** from the **Tasks** drop down menu. All of the below configuration options can be configured from the **Remote PC Properties**.

Enabling or Disabling a Remote PC in the Farm

By default a PC is enabled in the farm. When it is disabled, published applications and virtual desktops cannot be served from it.

To disable a PC from the farm untick the option **Enable Remote PC** from the **Properties** tab in the Remote PC Properties. Tick back (enable) any of the tick boxes to enable the computer back in the farm.



Properties Tab in Remote PC Properties

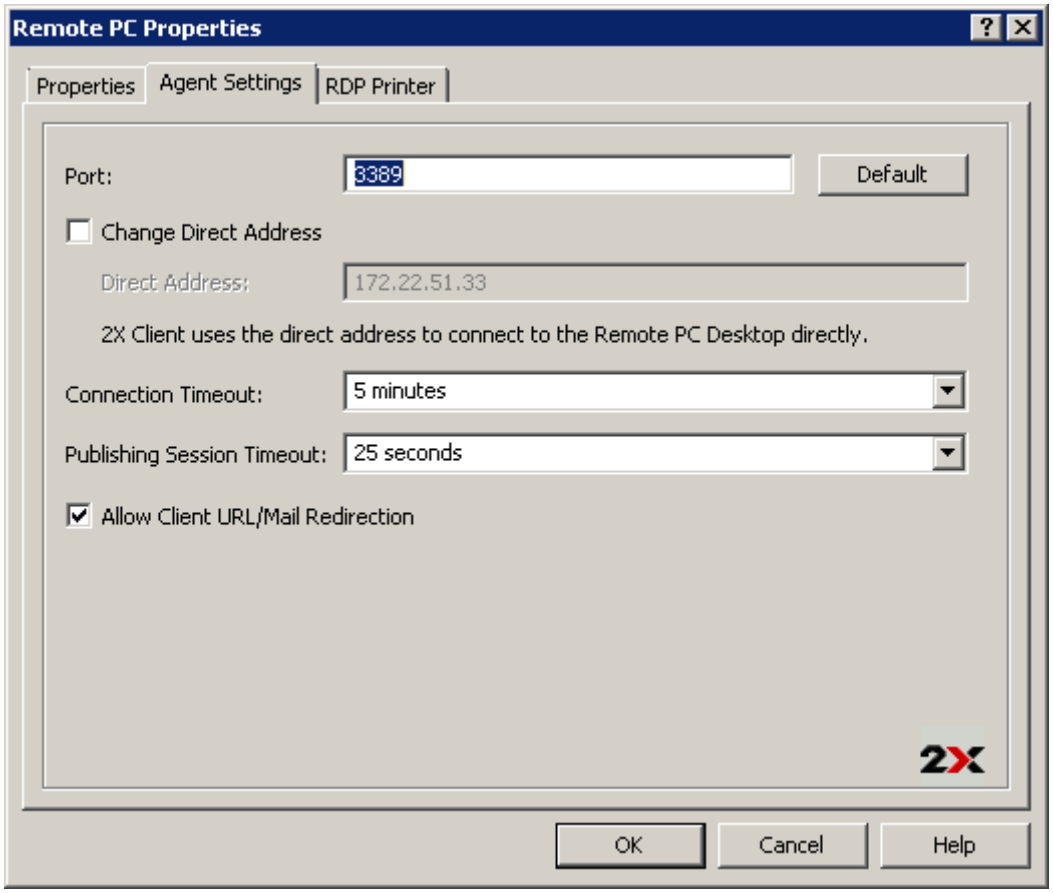
Configuring or Changing a Remote PC IP Address

From the **Properties** tab you can also change the remote PC IP address and add a description. The MAC address is also needed to automatically switch ON the PC when accessing resources from it.

Note: The Wake On Lan option should be enabled in the PC Bios options so the machine could be automatically turned on.

Configuring the Remote PC Agent

Each Remote PC in the farm has a 2X Agent installed to provide a connection between the 2X ApplicationServer XG and the PC. The agent can be configured from the **Agent Settings** tab in the pc properties.



Configuring Remote PC Agent Settings from Agent Settings Tab

Configuring the Remote Desktop Connection Port

Specify a different remote desktop connection port number in the **Port** input field if a non default port is configured on the pc.

Changing the Direct Address

This address is only used in Direct Connection mode and it could be an internal or external IP. To change the Direct Address of a remote PC tick the option **Change Direct Address** and specify the new address in the **Direct Address** input field.

Changing Connection Timeout

To increase the connection timeout of a remote PC select a value from the drop down menu **Connection** Timeout.

Changing the Session Timeout

To change the amount of time each session remains connected in the background after the user has closed the published application specify a new value in the **Publishing Session Timeout** input field. This option is used to avoid unnecessary reconnections with the pc.

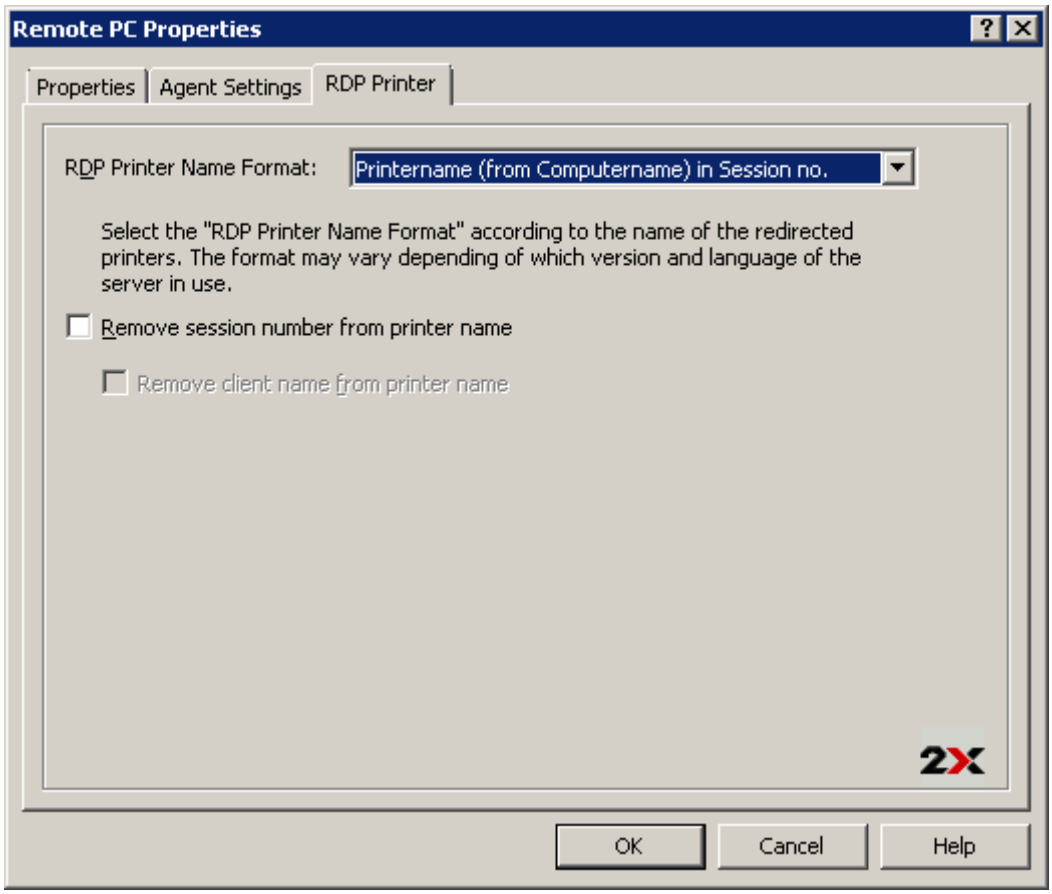
.

Configuring URL and Mail Redirect / Restricting Access

To allow http and mailto links to be opened using a local application on the client computer rather than the server's resources, enable the option **Allow Client URL/Mail Redirection**. To configure a list of URLs which should not be redirected navigate to the **URL Redirection** tab in the **Settings** node of a site.

Configuring RDP Printing for Remote PC

The **RDP Printer** tab allows you to configure the renaming format of redirected printers. The format may vary depending of which version and language of the server you are using.


Remote PC Properties
Properties
Agent Settings
RDP Printer
RDP Printer Name Format:
Printername (from Computername) in Session no.
Select the "RDP Printer Name Format" according to the name of the redirected printers. The format may vary depending of which version and language of the server in use.
Remove session number from printer name
Remove client name from printer name
2X
OK
Cancel
Help

Configuring RDP Printing from the RDP Printer Tab in Remote PC Properties

Set your RDP Printer Name Format specifically for the configured server by choosing any of the below options from the **RDP Printer Name Format** drop down menu:

- Printername (from Computername) in Session no.
- Session no. (computername from) Printername
- Printername (redirected Session no)

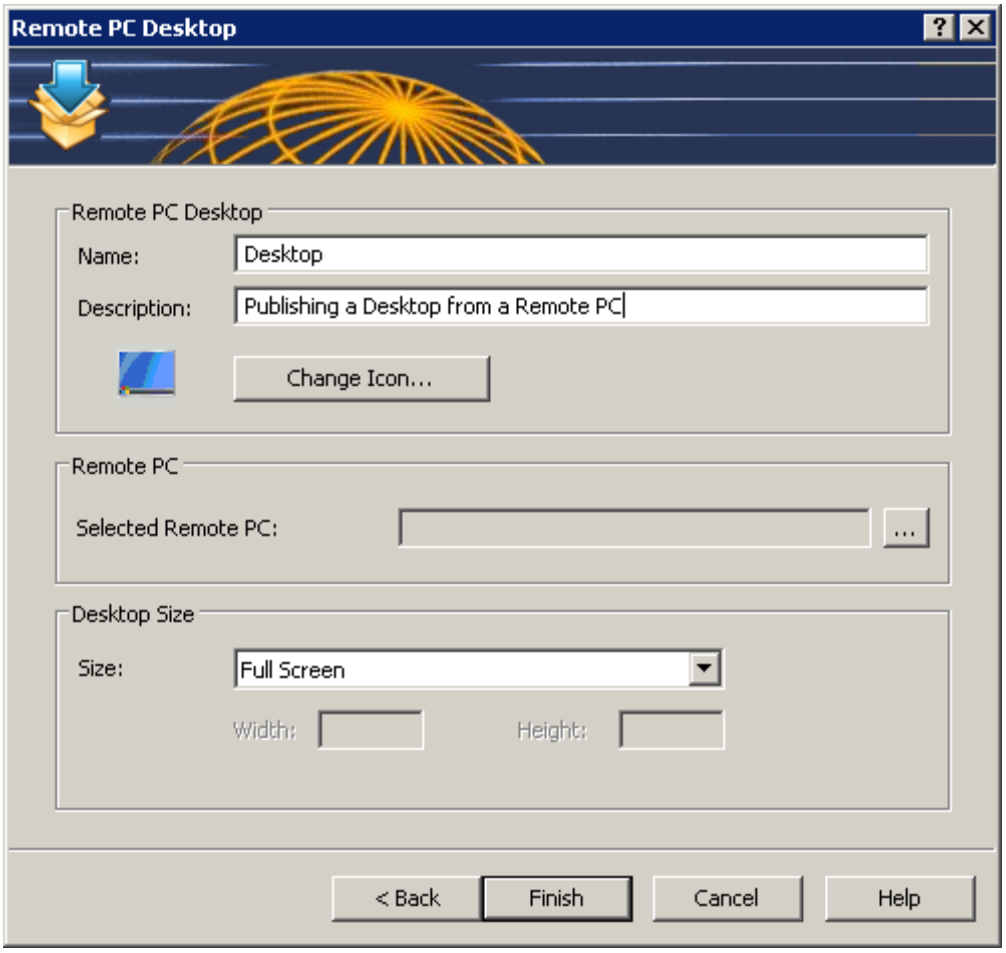
The other RDP Printing options available in the RDP Printer tab are:

- Remove session number from printer name
- Remove client name from printer name

Publishing a Desktop from a Remote PC

To publish a desktop from a terminal server follow the below procedure:

1. Click **Publishing** from the system menu and click the **Desktop** icon from the top navigation bar.
2. Select **Remote PC Desktop** in the first step of the wizard and click **Next**.
3. In the second step of the wizard specify a **Name** and **Description** in the **Desktop** section. From the same section you can also configure an icon by clicking on the **Change Icon** button.
4. Click the **Browse** button in the **Remote PC** section to specify from which Remote PC the desktop should be published.
5. From the **Desktop Size** section you can specify the resolution of the desktop.



Configuring a Desktop to be Published from a Remote PC

6. Once ready click **Finish** to publish the desktop.

Publishing an Application from a Remote PC

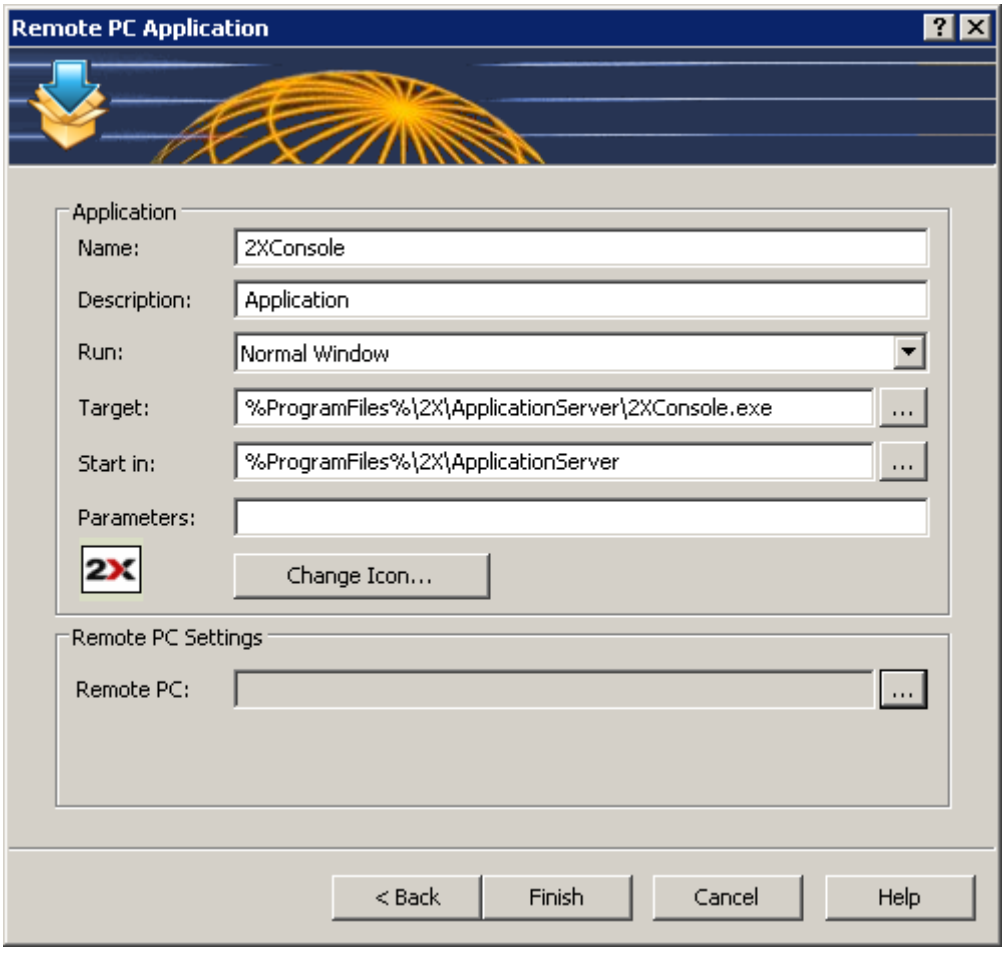
To publish an application from a terminal server follow the below procedure:

1. Select the **Publishing** category from the system menu and click the **Application** icon from the top navigation bar.
2. Select **Remote PC** in the first step of the wizard and click **Next**.
3. From Remote PCs you can only publish **Single** Application. Therefore in the second step of the wizard click **Next**.

4. In the third step of the wizard you have to configure the application.

Note: Use the **Browse** button next to the **Target** input field to browse to the application executable. Once the application is selected, all other configuration options will be automatically populated. If you would like to configure all application entries manually, follow the below procedure.

5. Enter a **Name** and **Description** in the **Application** section.
6. From the **Run** drop down menu specify if the application should run in a normal window, maximized or minimized.
7. Specify the path where the application executable is in the **Target** input field by clicking the **browse** button and browse to the executable. Use Windows environment variables if you are manually specifying the path.
8. The **Start In** input field will be automatically populated. To specify a different folder from where the application should be launched click the **Browse** button. A different folder might be specified if for example the application needs to use files from another location to run. In such case, specify such folder location so the published application will be able to locate them upon it being launched.
9. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application upon being launched.
10. You can change the icon for the published application by clicking the **Change Icon** button.
11. Click the **Browse** button in the **Remote PC Settings** section to select a remote PC from the list from which the application should be published.



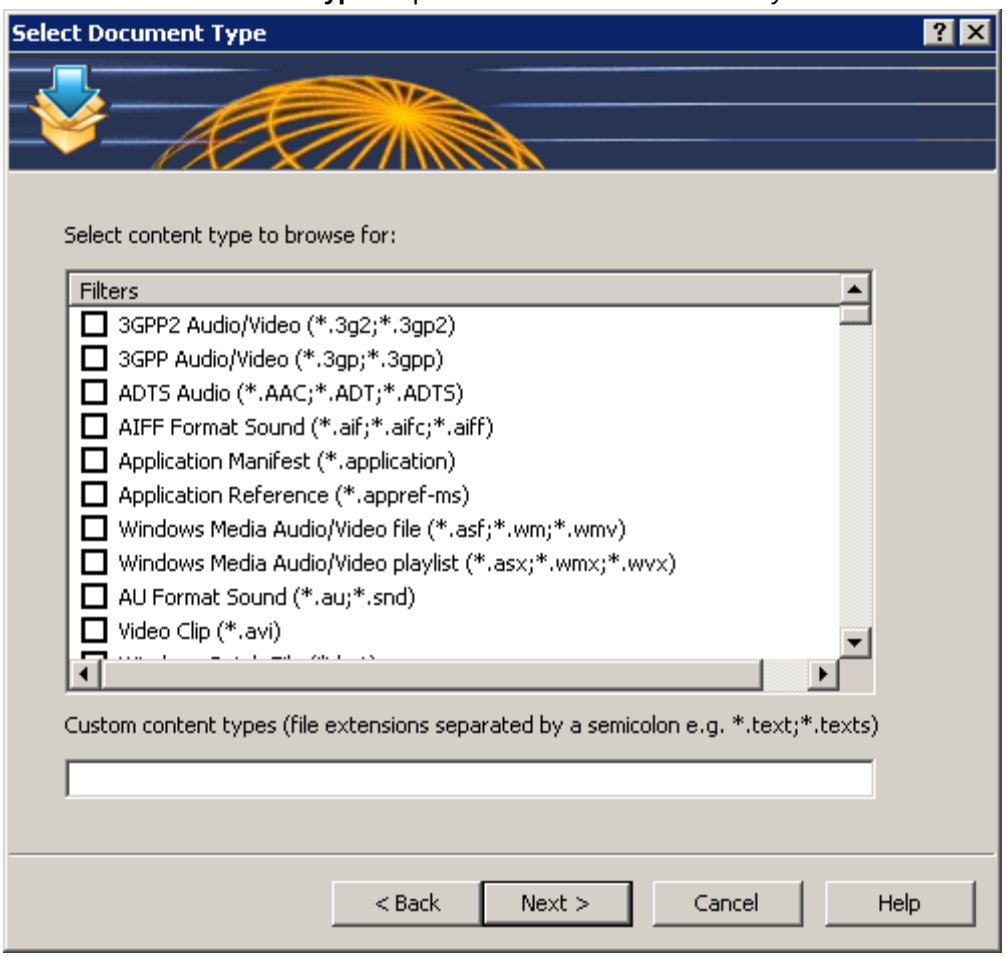
Configuring an Application to be Published from a Remote PC

12. Once ready click **Finish** to publish the application.

Publishing a Document from a Remote PC

To publish a document from a terminal server follow the below procedure:

1. Click the **Publishing** category and click the **Document** icon from the top navigation bar.
2. Select **Remote PC** in the first step of the wizard and click **Next**.
3. In the second step specify the content type of the document you want to publish. You can select the content type from the predefined list or specify a custom content type from the **Custom content types** input field. Click **Next** once ready.

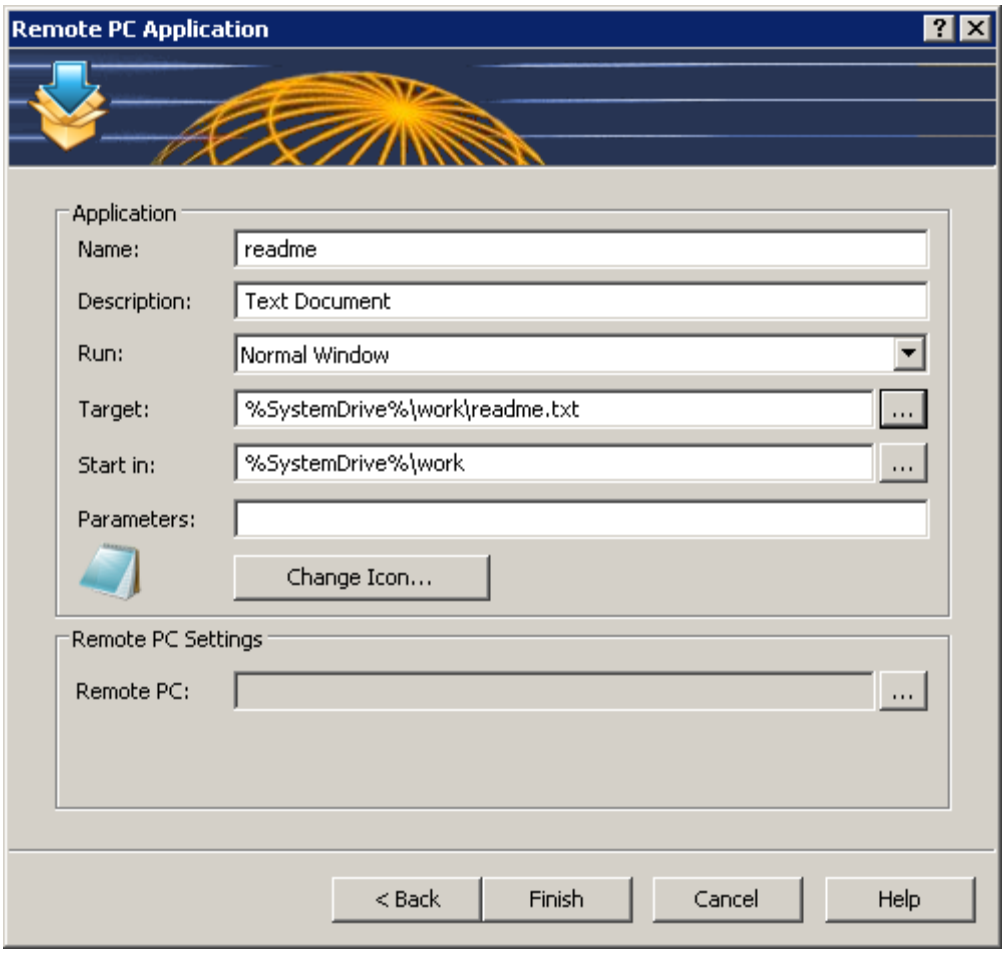


Configuring a Content Type for the Document

Note: In the third step of the wizard use the **Browse** button next to the **Target** input field to browse to the document. Once the document is selected, all other configuration options will be automatically populated. If you would like to configure all entries manually, follow the below procedure.

4. In the third step of the wizard enter a **Name** and **Description** for the document in the **Application section**.
5. From the **Run** drop down menu specify if the document should run in a normal window, maximized or minimized.
6. Specify the path where the document is in the **Target** input field by clicking the **browse** button and browse to the document. Use Windows environment variables if you are manually specifying the path.

7. The **Start In** input field will be automatically populated. To specify a different folder from where the document should be launched click the **Browse** button.
8. (Optional) In the **Parameters** input field you can specify parameters which have to be passed to the application upon being started and you can change the icon for the published document by clicking the **Change Icon** button.
9. Click the **Browse** button in the **Remote PC Settings** section to select a remote PC from the list from which the document should be published.



Configuring a Document to be Published from a Remote PC

10. Once ready click **Finish** to publish the document.

Publishing and Filtering

Introduction

Publishing is one of the fundamental uses and features of the 2X ApplicationServer. The 2X ApplicationServer can be used to publish:

- Applications
- Folders
- Desktops
- Predefined Applications
- Documents

Managing Published Applications

Publishing an Application

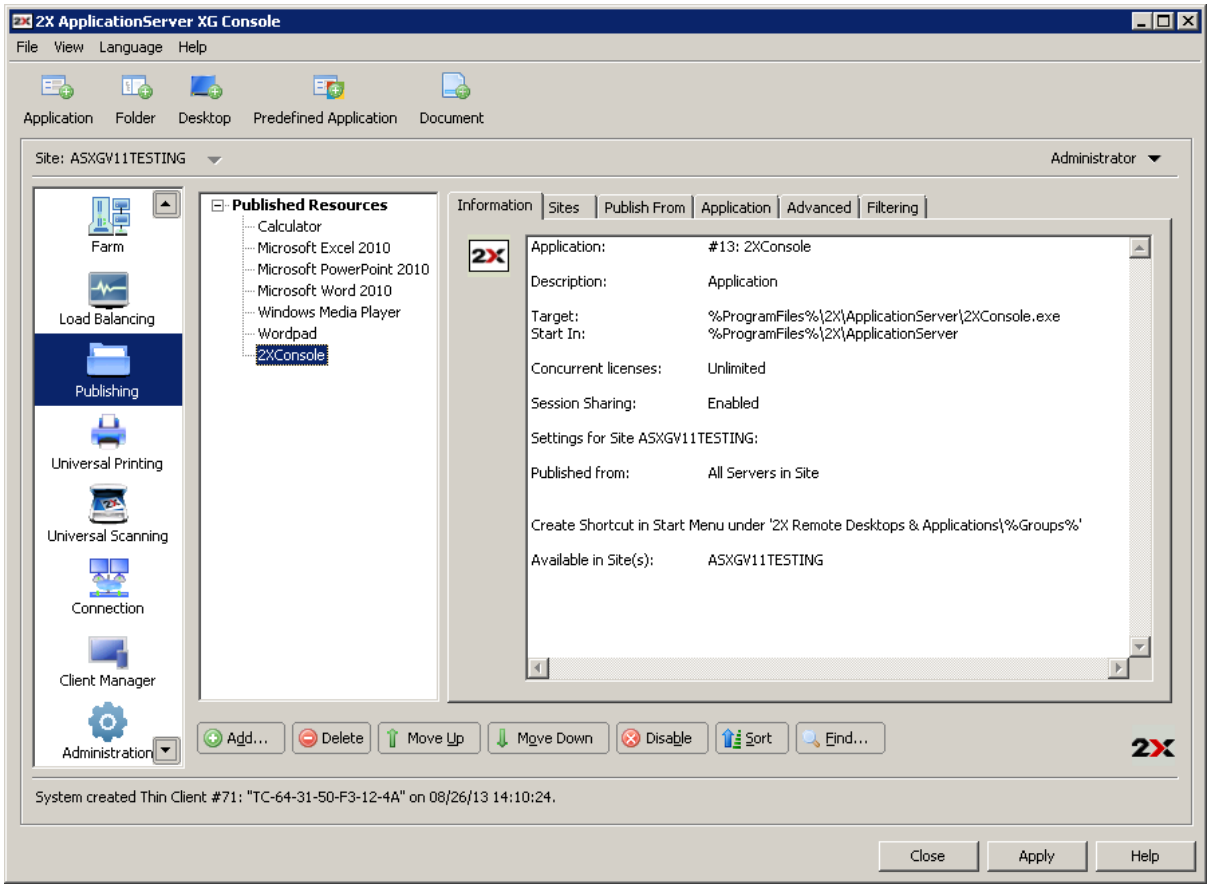
To publish an application that can be accessed by users on the network, you can follow any of the following procedures:

- **Publishing an Application from a Terminal Server** from page 31
- **Publishing an Application from a Remote PC** page 62
- **Publishing an Application from a Guest** page 52

Configuring a Published Application

When publishing an application through the wizard you have to specify several application parameters such as the name, the executable path etc. These options and several others can also be modified once the application has been published.

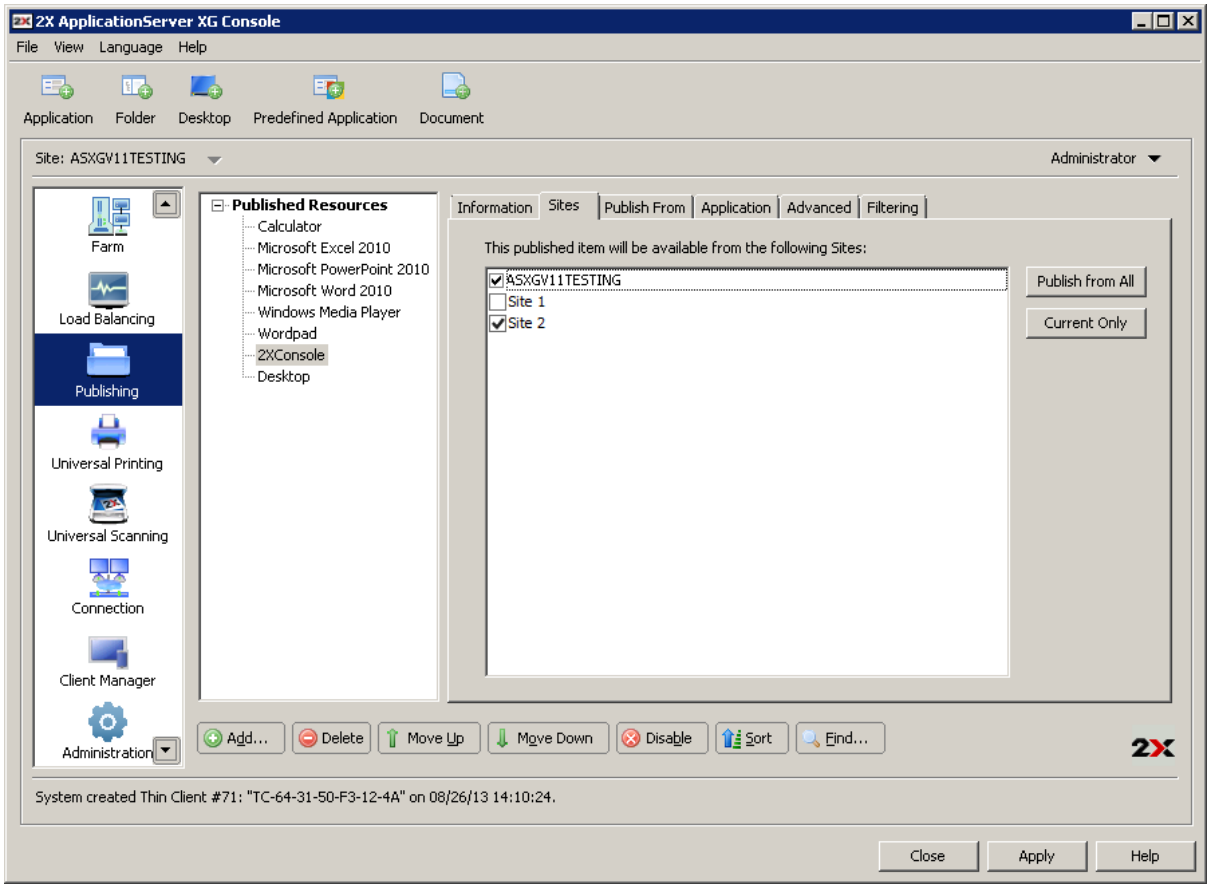
To modify a published application, select the application from the **Published Resources** tree in the **Publishing** category.



Configuring a Published Resource

Configuring the Sites through which a Published Application is Available

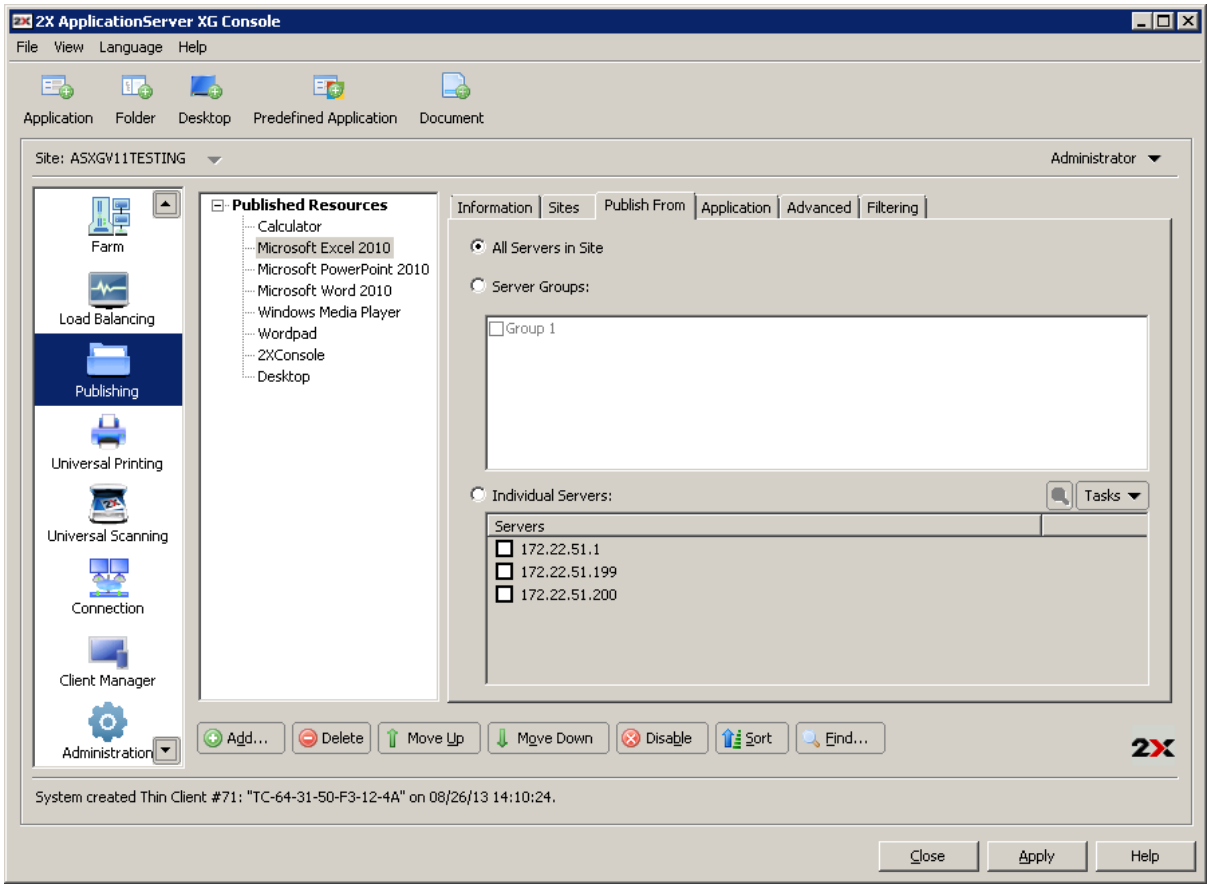
By default a published application is available through all the sites. To restrict access to a specific site or group of sites, select the list of sites from the **Sites** tab in the published application options.



Configuring the Sites a Published Application is Available Through

Configuring from which Servers the Application is Published From

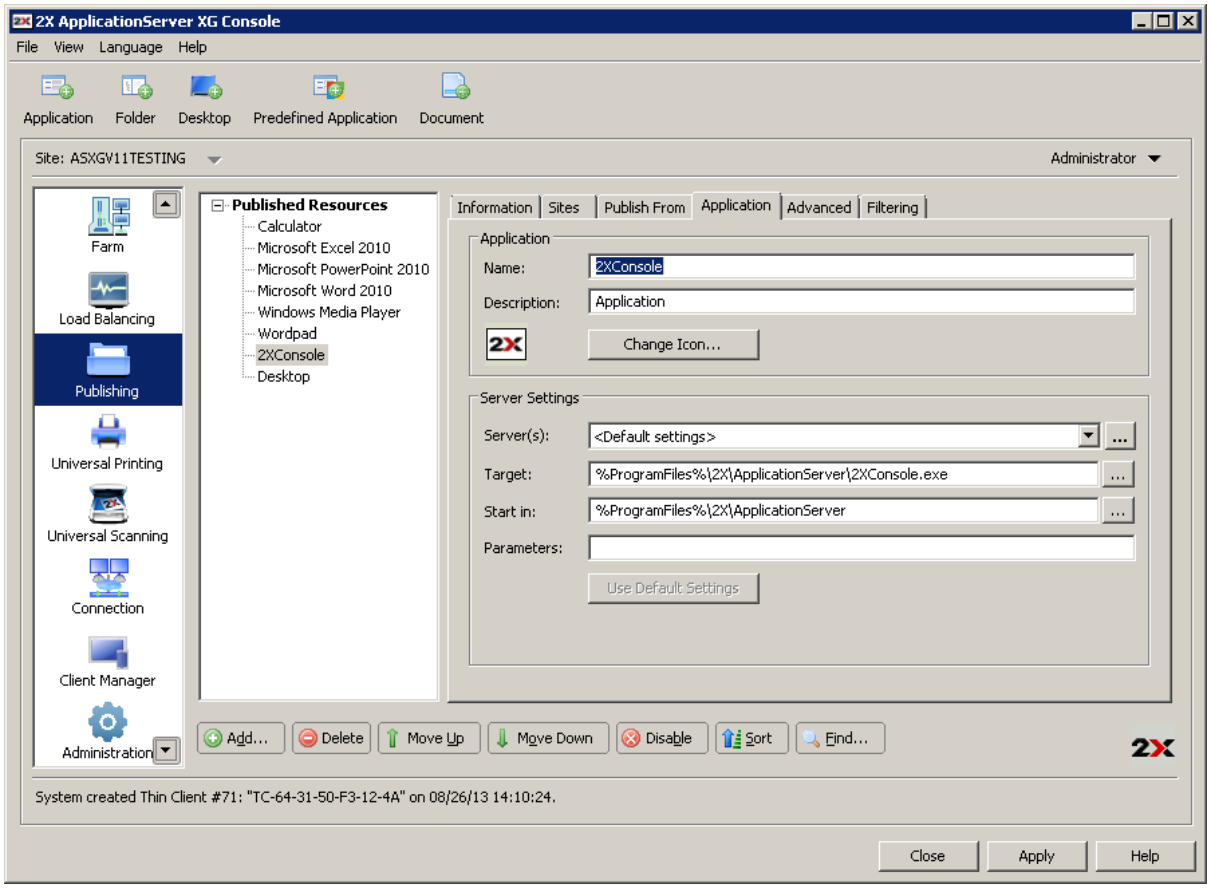
From the **Publish From** tab you can specify from which terminal servers should the published application be published as seen in the below screenshot.



Configuring from which Servers a Published Application is Available

Configuring Server Specific Application Settings

By default the settings configured in the **Target** (application path), **Start In** and **Parameters** apply to all servers an application is published from. In case the application is installed in a different path on one of the servers, use the **Server(s)** drop down menu in the **Application** tab to specify new settings in the **Target**, **Start In** and **Parameter** input fields specific for that server.

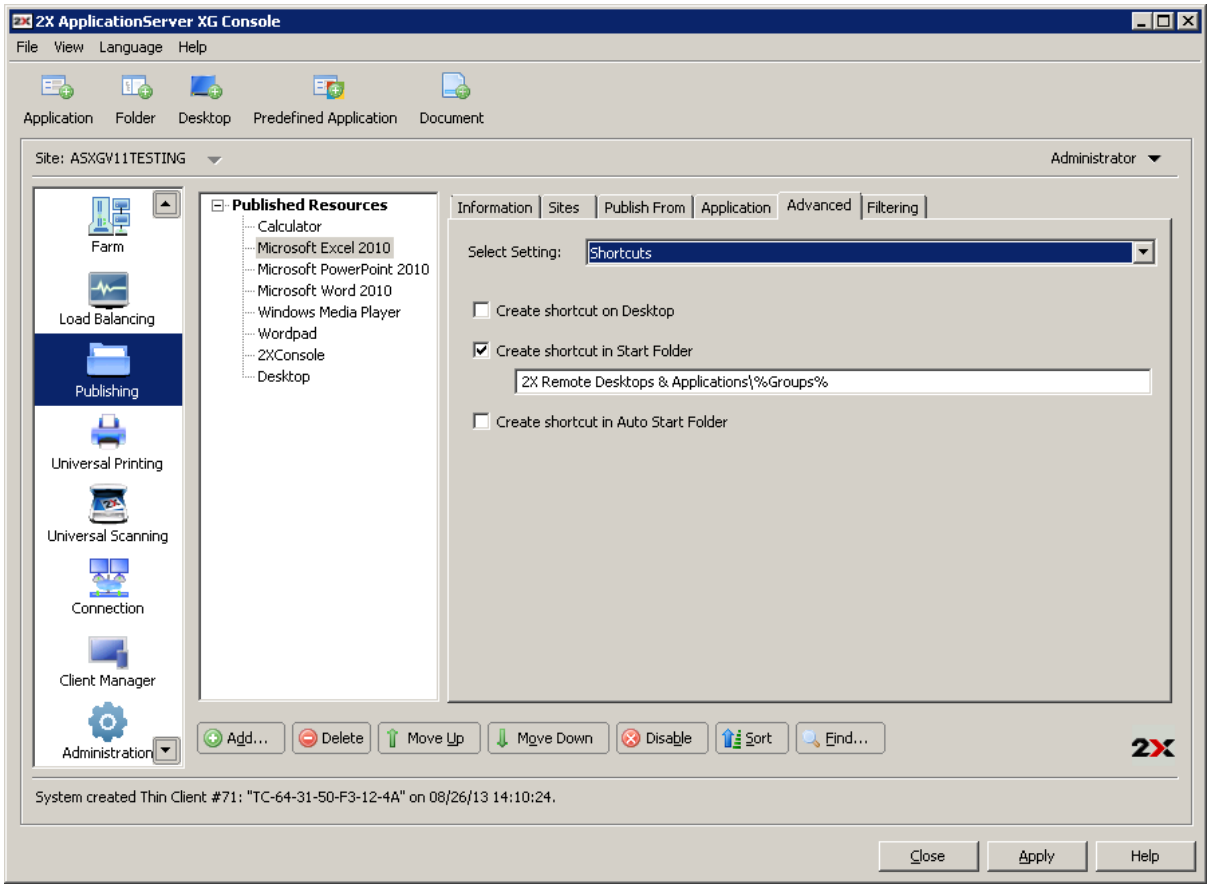


Configuring Server Specific Settings for a Published Application

Configuring Shortcuts Options for a Published Application

Click the **Advanced** tab in the application settings and select **Shortcuts** from the **Select Setting** drop down menu to enable the creation of shortcuts on the user's desktop, shortcuts in the start folder with relative folder and shortcut in the Auto start folder. When the Auto start shortcut is enabled the application will be started when the Operating system the client is running is started.

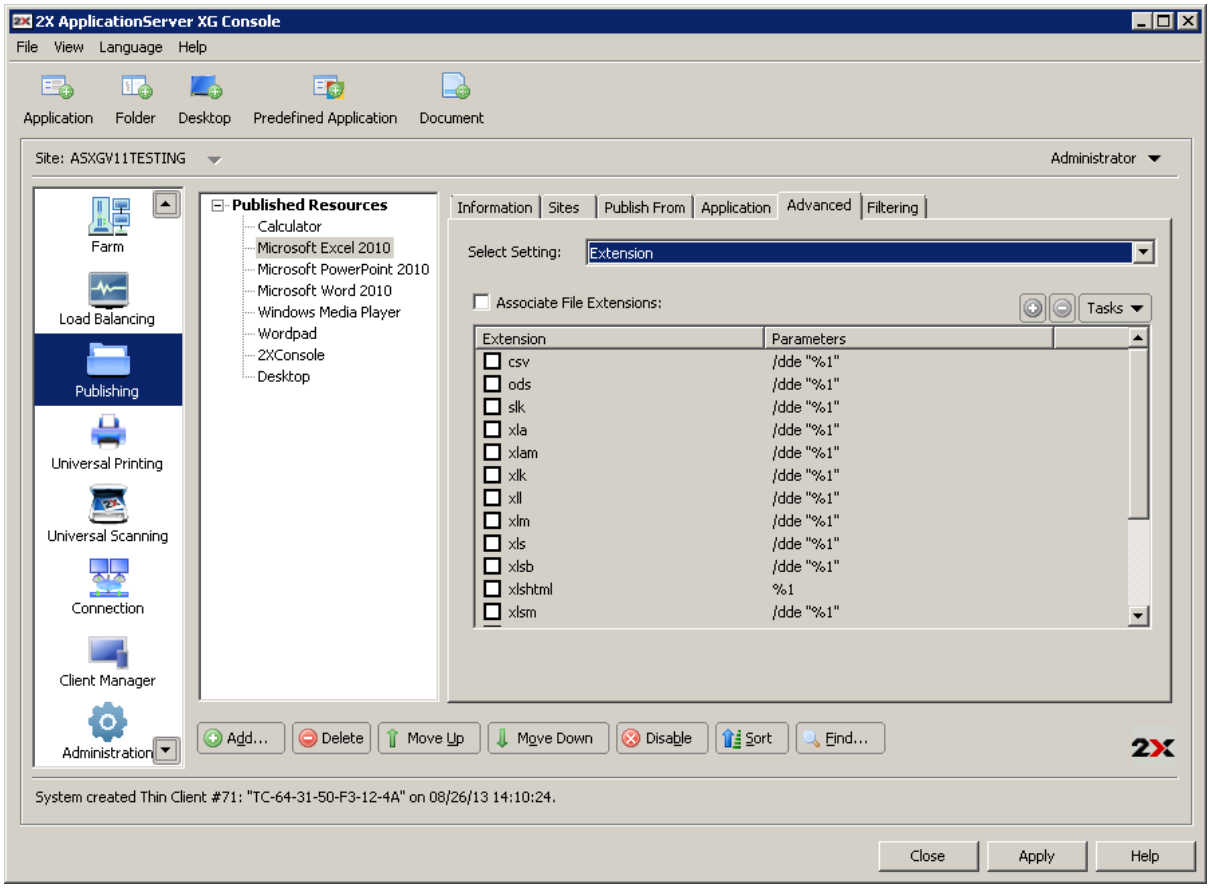
Note: This option is not available on all operating systems



Configuring 2X OS Shortcut Options for a Published Application

Configuring File Extension Associations

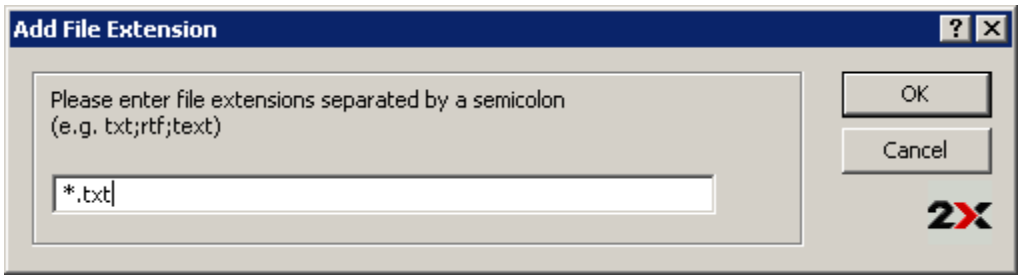
To modify file extension association for a particular published application, click the **Advanced** tab in the application settings and select **Extensions** from the **Select Setting** drop down menu.



Configuring File Extension Associations for a Published Application

Note: A list of typically associated file extensions is automatically generated once an application is published. If you would like to modify the preconfigured list and add, remove or modify an existing entry, tick the option **Associate File Extensions**.

To add a new extension to the list, click **Add** from the **Tasks** drop down menu and specify the extension as shown in the below screenshot.



Configuring a new File Extension

To modify an extension's parameters, highlight the extension and click **Properties** from the **Tasks** drop down menu.

Configuring Licensing Options for Published Applications

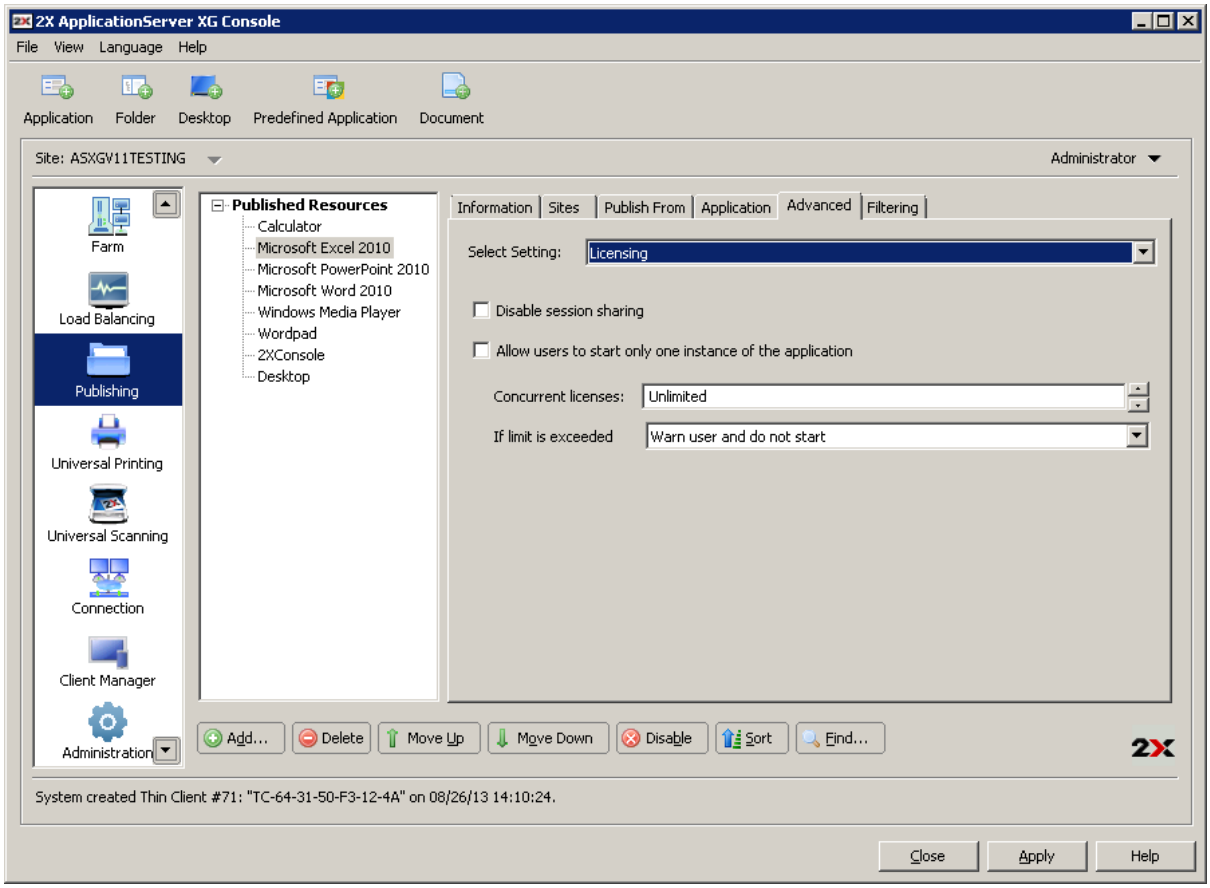
Click the **Advanced** tab in the application settings and select **Licensing** from the **Select Setting** drop down menu to configure any of the below licensing options:

Disable session Sharing: If this option is enabled, it allows you to isolate the published application to one session. Therefore if the same application is launched twice, the multiple instances of the application will run in the same isolated session.

Allow users to start only one instance of the application: If this option is enabled, a user can only launch a single instance of the application.

Concurrent Licenses: Use this option to specify the maximum number of concurrent instances the application can run. E.g. if the license of the application allows you to only run 10 instances of the application, set the **Concurrent licences** option to 10 so once such limit is reached, other users cannot initiate other instances.

If limit is exceeded: From this drop down menu you can specify what action should the 2X ApplicationServer XG take in case any of the above licensing configured limits has been exceeded.

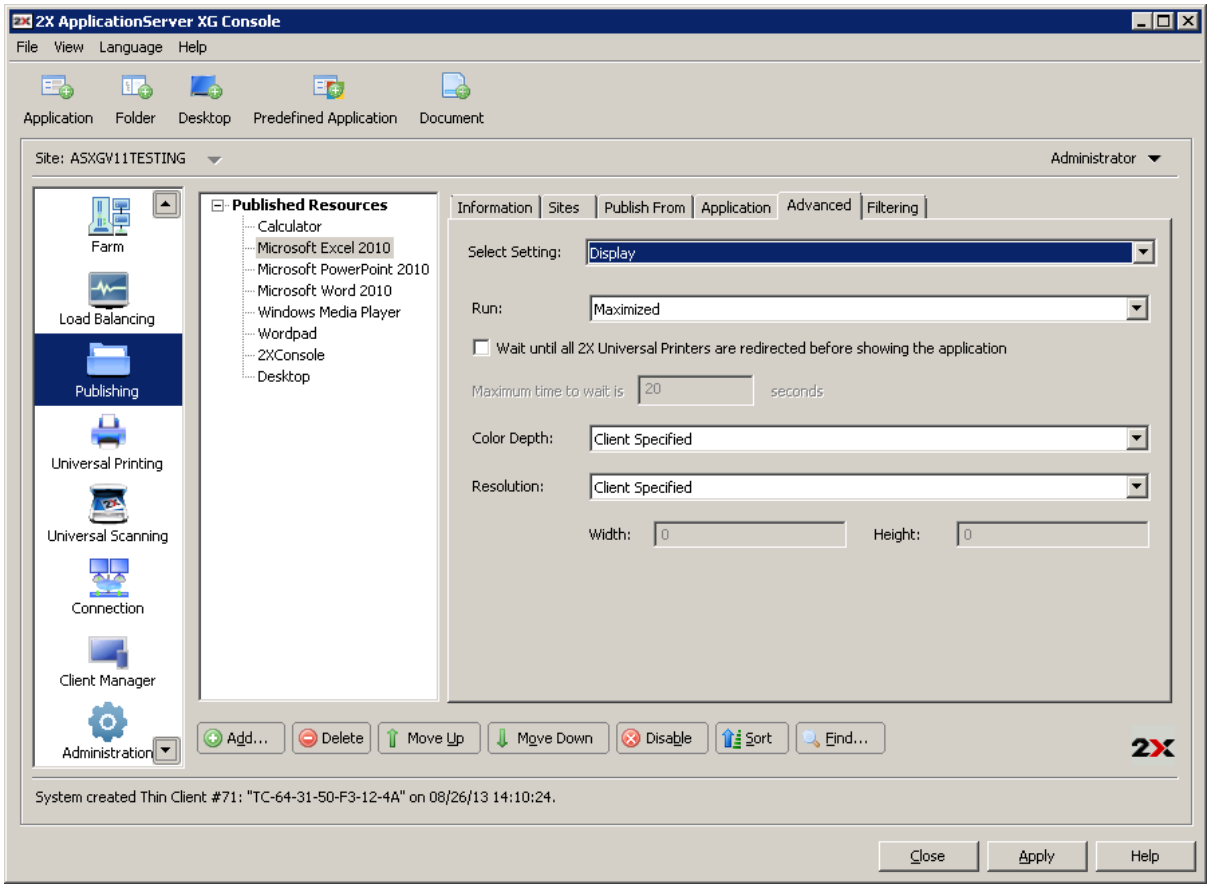


Configuring Licensing Options of a Published Application

Configuring Display Settings for a Published Application

Click the **Advanced** tab in the application settings and select **Display** from the **Select Setting** drop down menu to configure the color depth of the published application, resolution and width and height. If these options are left as default, the client specified options will take over.

From this section you can also enable the option to wait for the 2X Universal Printers to be redirected before the application is loaded. When enabling this option you can also configure the maximum time to wait in seconds for the 2X Universal Printers to be redirected.



Configuring Display Options of a Published Application

Managing Published Desktops

Publishing a Desktop

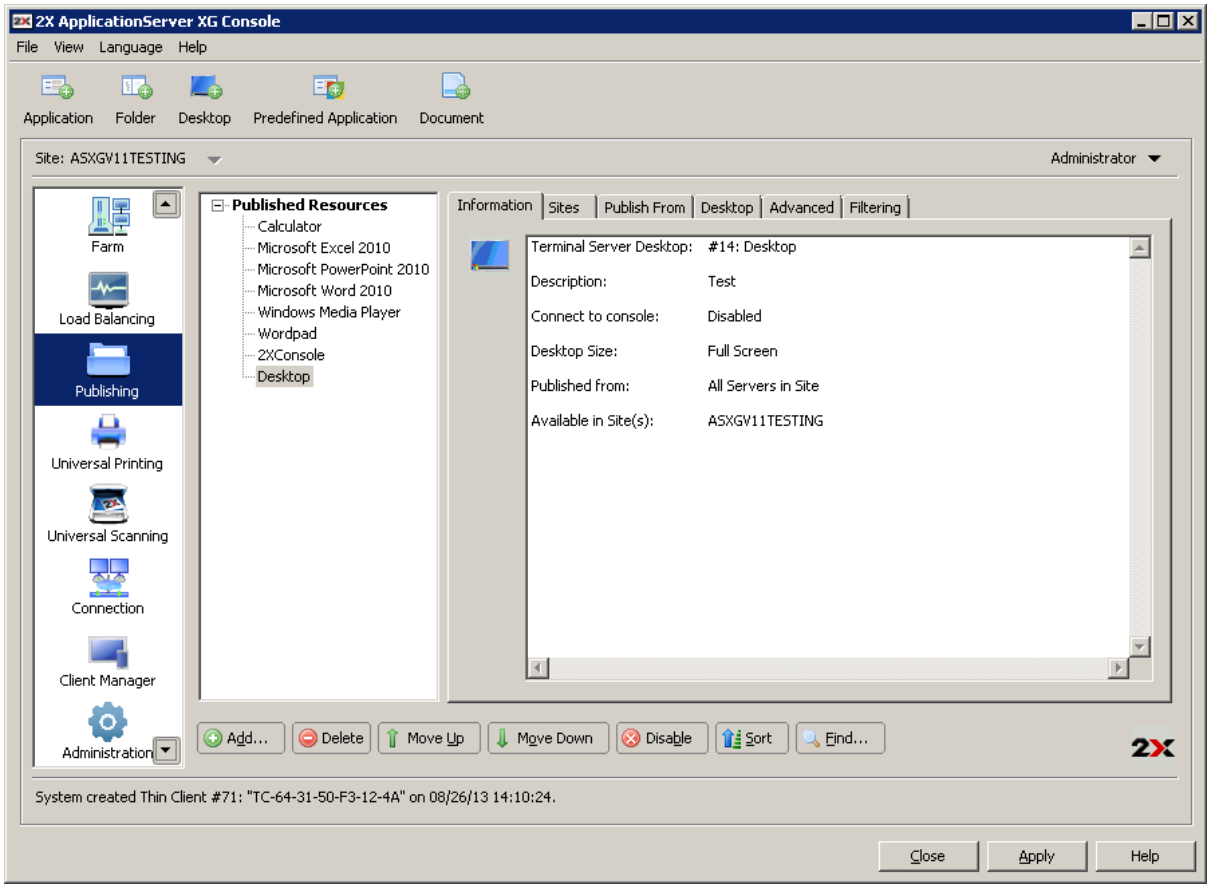
To publish a desktop that can be accessed by users on the network, you can follow any of the following procedures:

- Publishing a Desktop from a Terminal Server on page 29
- Publishing a Desktop from a Remote PC on page 62
- Publishing a Virtual Desktop from a Guest on page 50

Configuring a Published Desktop

When publishing a desktop through the wizard you have to specify all the desktop settings, such as display size etc. These options and several others can also be modified once the desktop has been published.

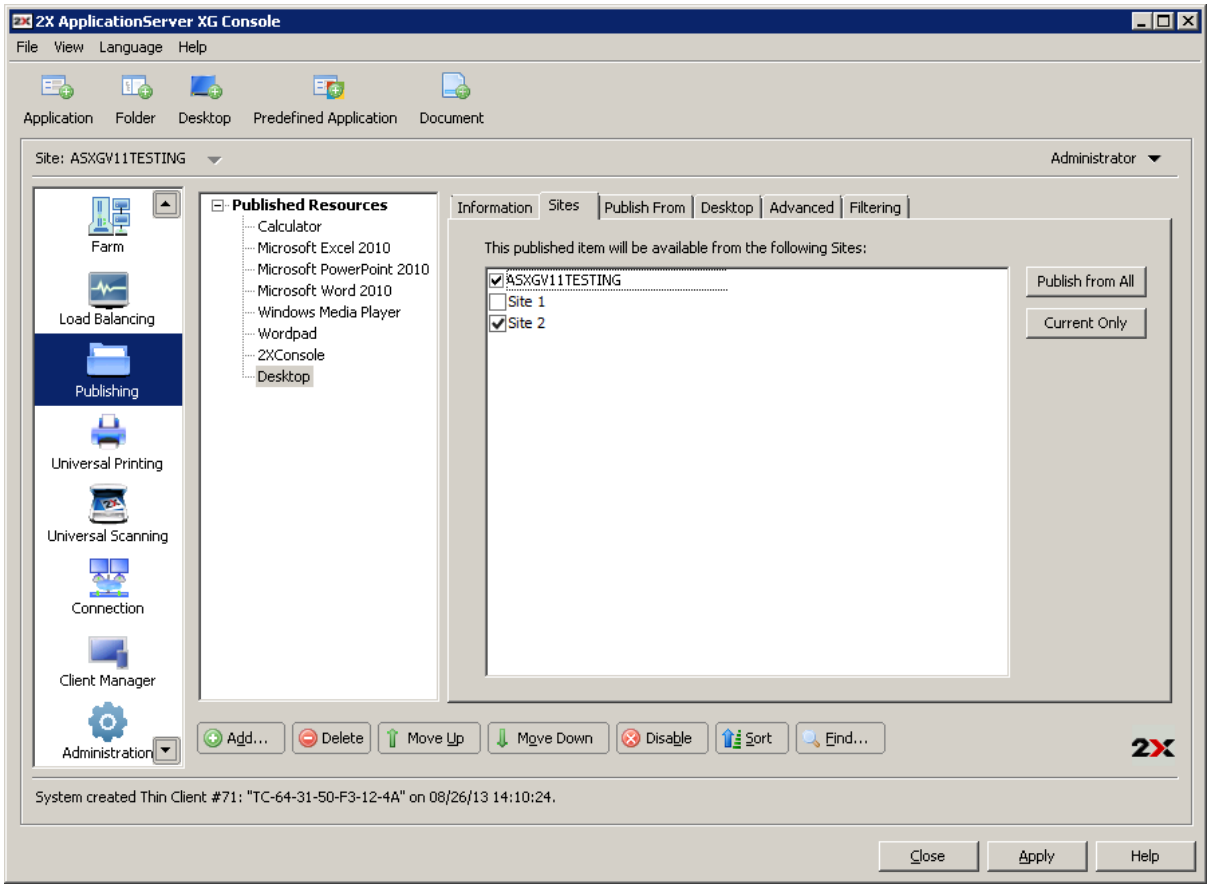
To modify a published desktop, select the desktop from the **Published Resources** tree in the **Publishing** category.



Configuring a Published Desktop

Configuring the Sites through which a Published Desktop is Available

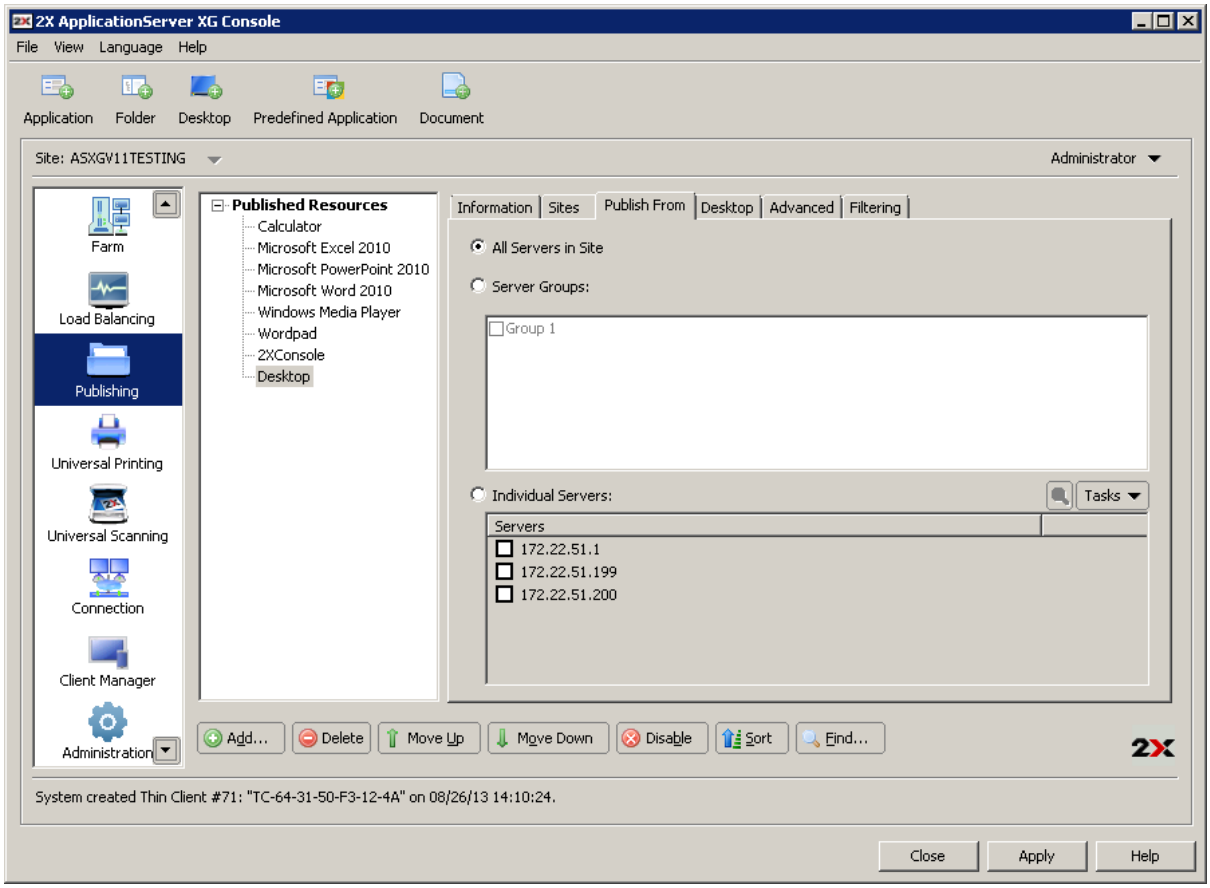
By default a published desktop is available through all the sites. To restrict access to a specific site or group of sites, select the list of sites from the **Sites** tab in the published desktop options.



Configuring the Sites a Published Desktop is Available Through

Configuring from which Servers the Desktop is Published From

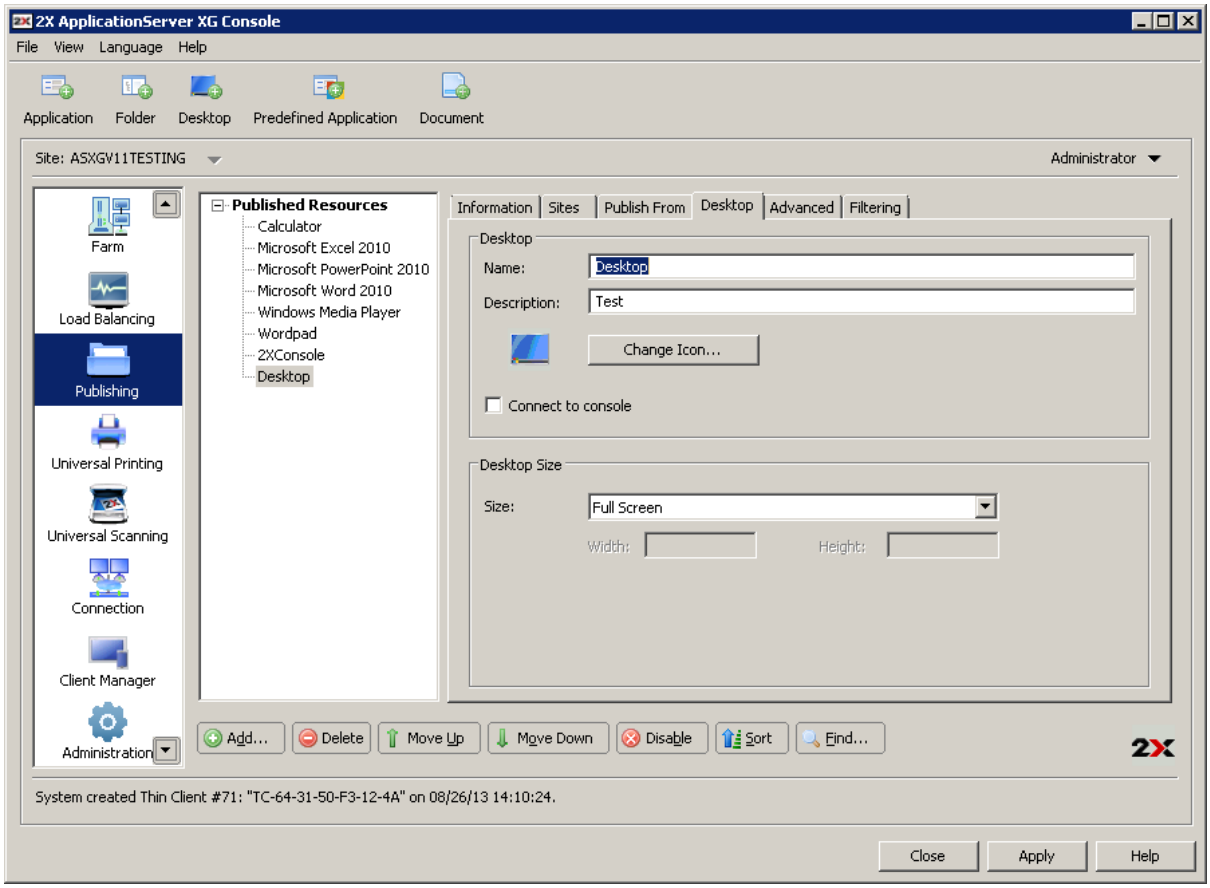
From the **Publish From** tab you can specify from which terminal servers should the published desktop be published as seen in the below screenshot.



Configuring the Servers a Published Desktop is Published From

Configuring Desktop Resolution and Other Properties

Click the **Desktop** tab to configure the desktop name, description, icon and resolution. From the **Desktop** tab you can also configure the virtual desktop to allow users to allow to the console of a server rather than a virtual instance.

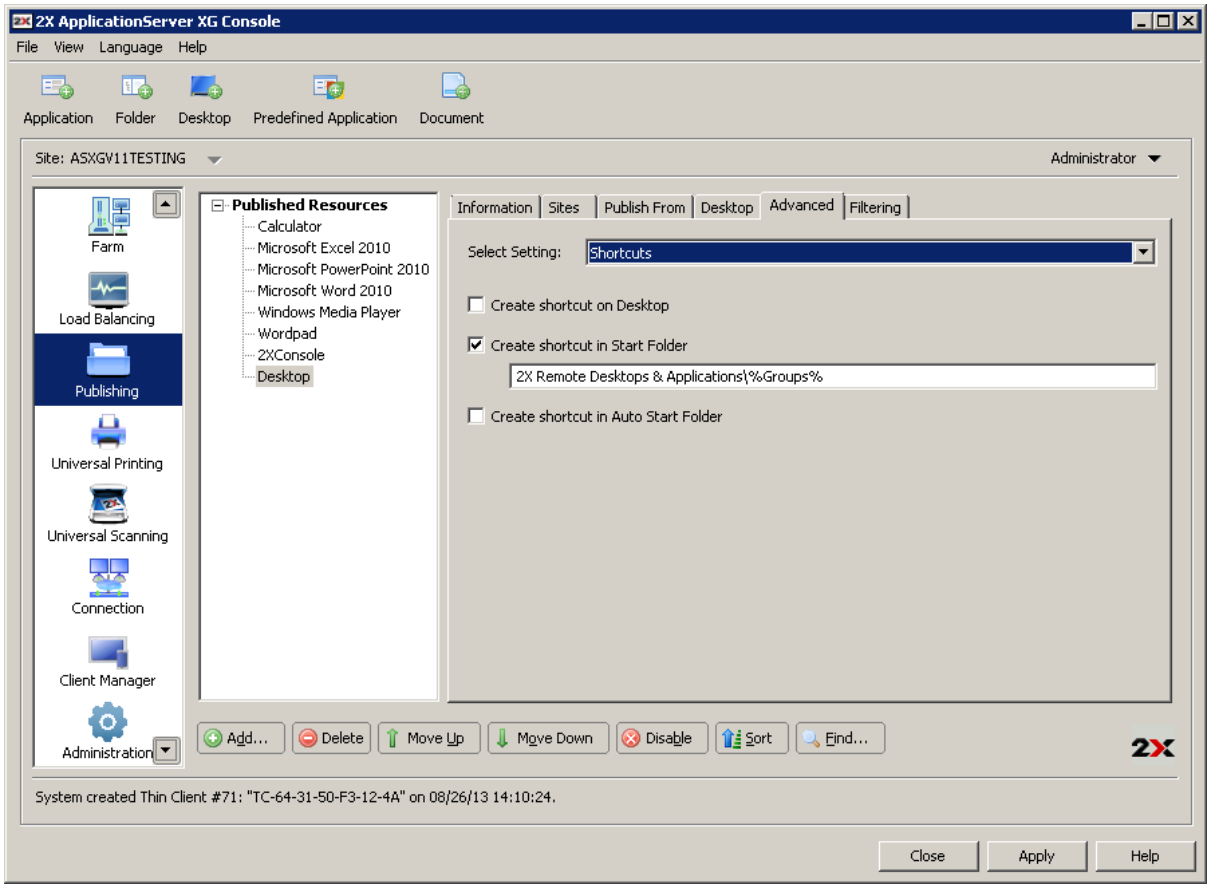


Configuring the Desktop Resolution

Configuring Shortcuts Options for a Published Desktop

Click the **Advanced** tab in the application settings and select **Shortcuts** from the **Select Setting** drop down menu to enable the creation of shortcuts on the user's desktop, shortcuts in the start folder with relative folder and shortcut in the Auto start folder. When the Auto start shortcut is enabled the application will be started when the Operating system the client is running is started.

Note: This option is not available on all operating systems.



Configuring the 2X OS Shortcut Options for a Published Desktop

Managing Published Documents

Publishing a Document

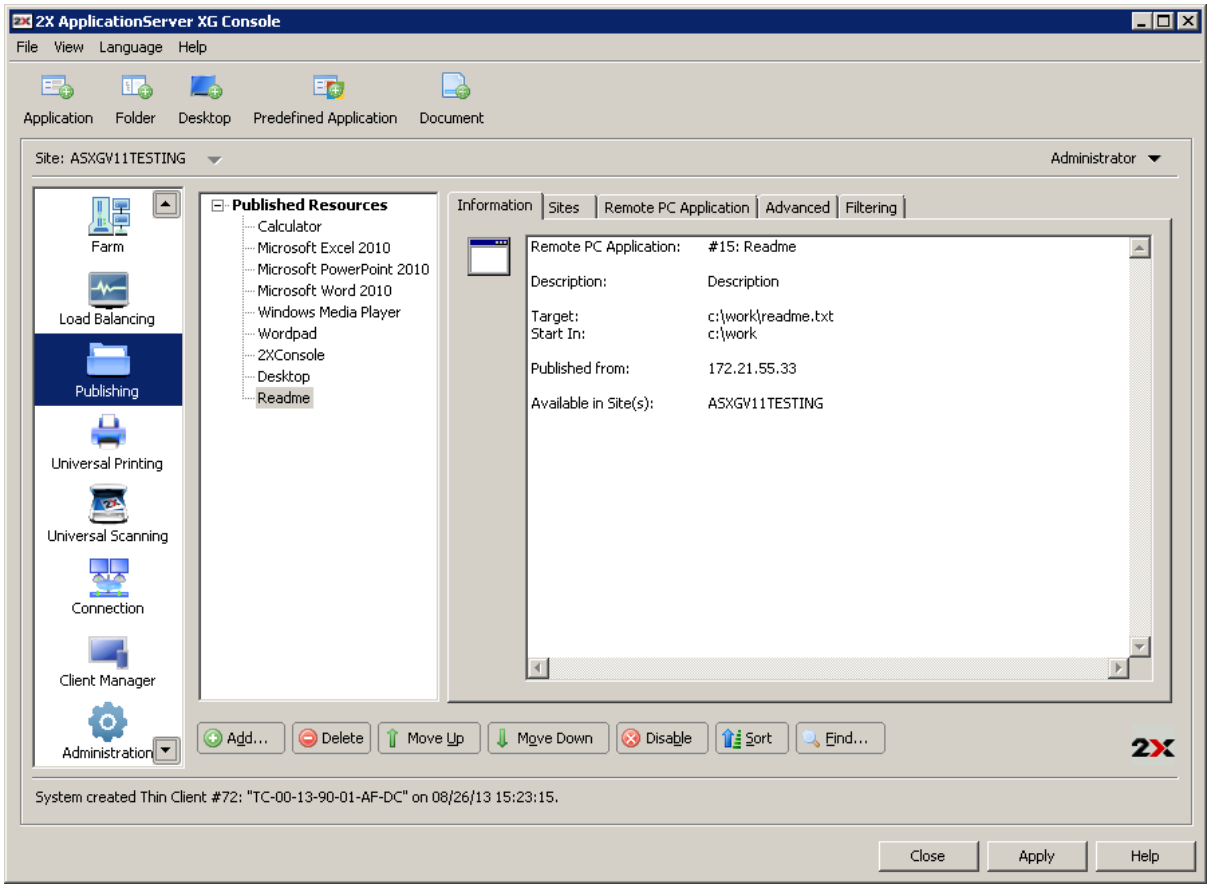
To publish a document that can be accessed by users on the network, you can follow any of the following procedures:

- Publishing a Document from a Terminal Server on page 33
- Publishing a Document from a Remote PC on page 64
- Publishing a Document from a Guest_Publishing_a_Document_2 on page 53

Configuring a Published Document

When publishing a document using the wizard you have to specify all the document settings, such as where it is stored etc. These options and several others can also be configured once the document has been published.

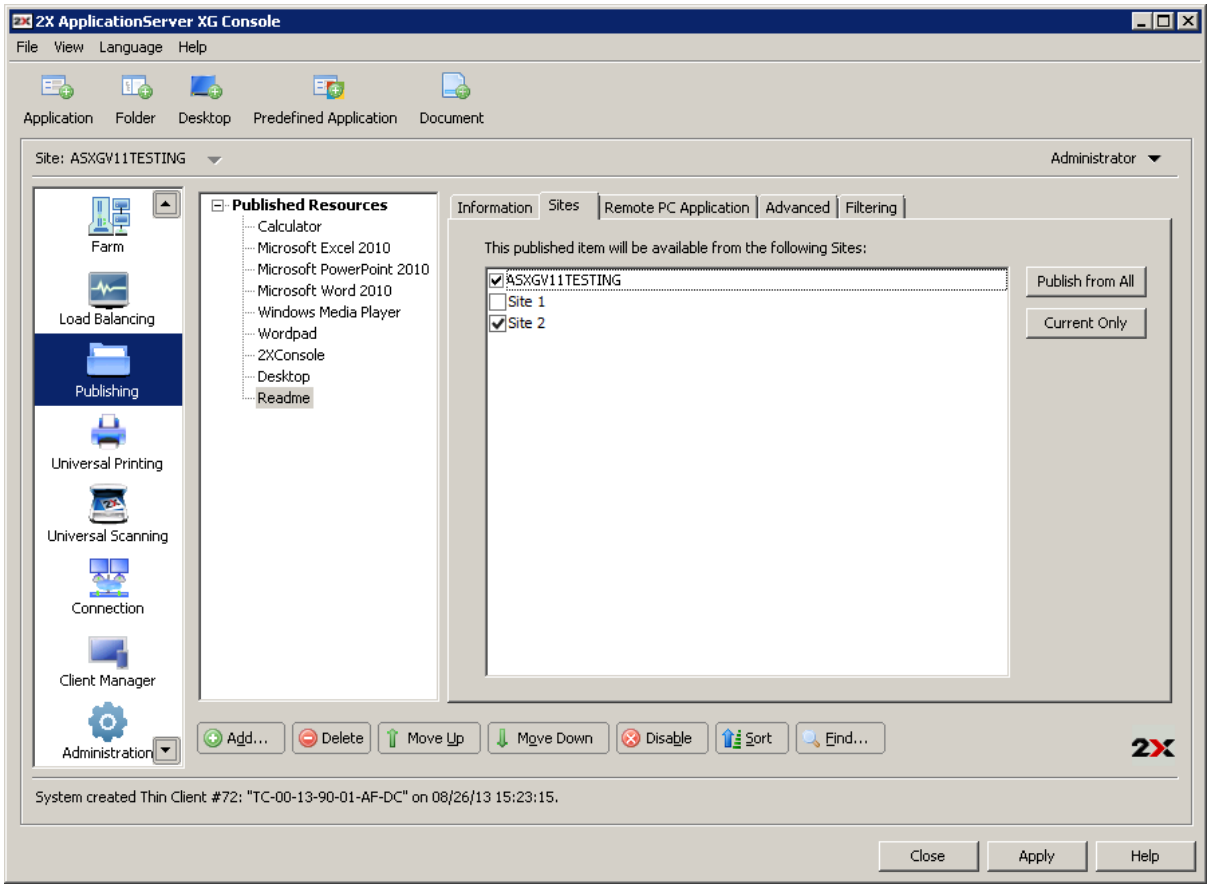
To modify a published document, select the published document from the **Published Resources** tree in the **Publishing** category.



Configuring a Published Document

Configuring the Sites through which a Published Document is Available

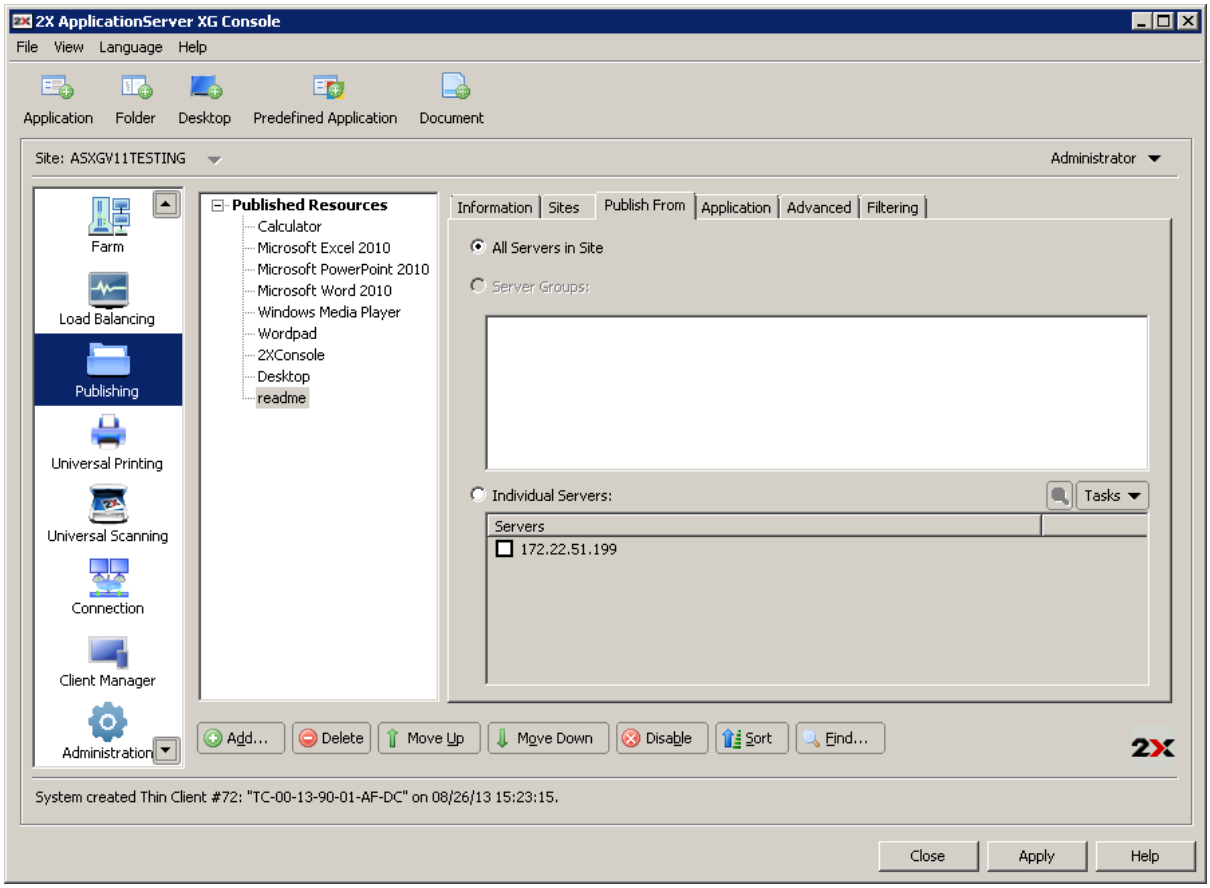
By default a published document is available through all the sites. To restrict access to a specific site or group of sites, select the list of sites from the **Sites** tab in the published document options.



Configuring the Sites a Published Document is Available Through

Configuring from which Servers the Document is Published From

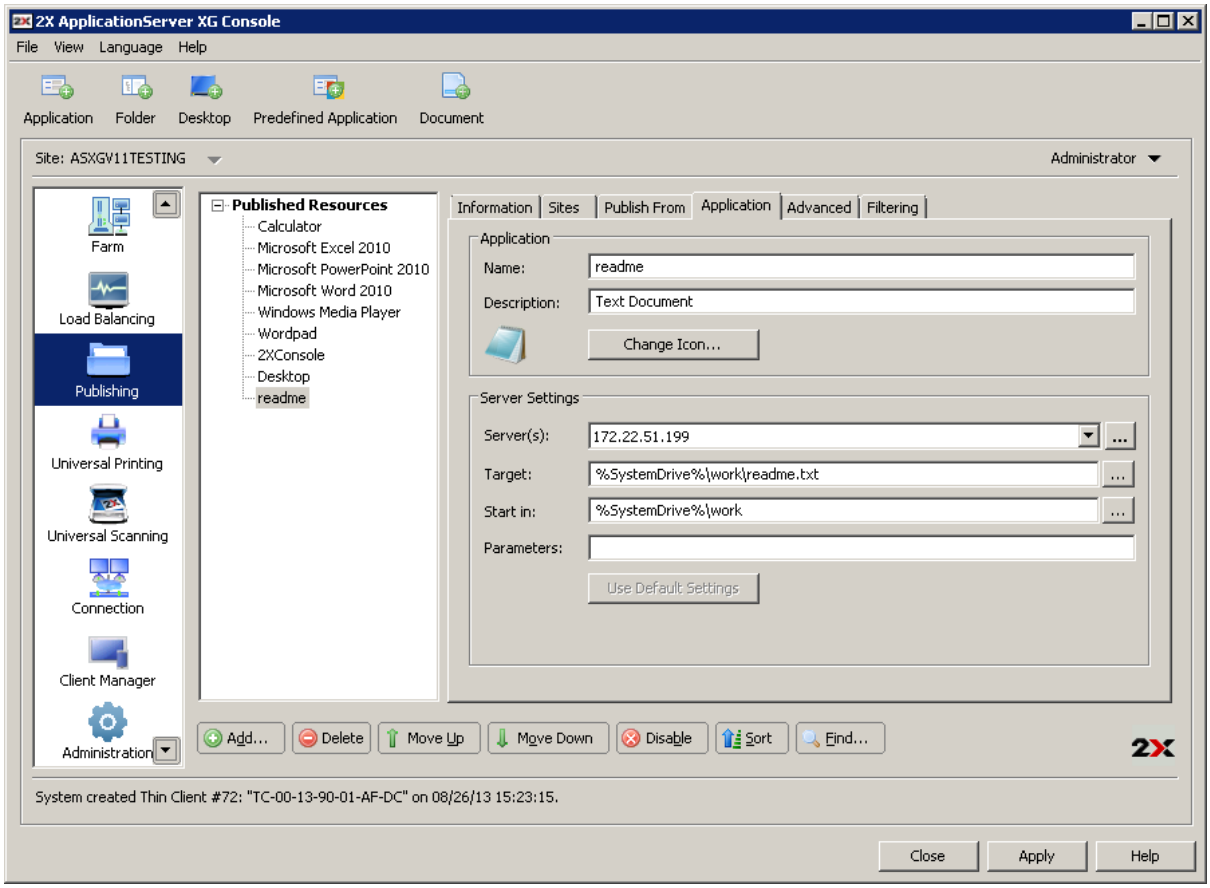
From the **Publish From** tab you can specify from which terminal servers should the published document be published as seen in the below screenshot.



Configuring the Servers a Published Document is Published From

Configuring Server Specific Document Settings

By default the settings configured in the **Target** (application path), **Start In** and **Parameters** apply to all servers a document is published from. In case the document is saved in a different path on one of the servers, use the **Server(s)** drop down menu in the **Application** tab to specify new settings in the **Target**, **Start In** and **Parameter** input fields specific for that server.



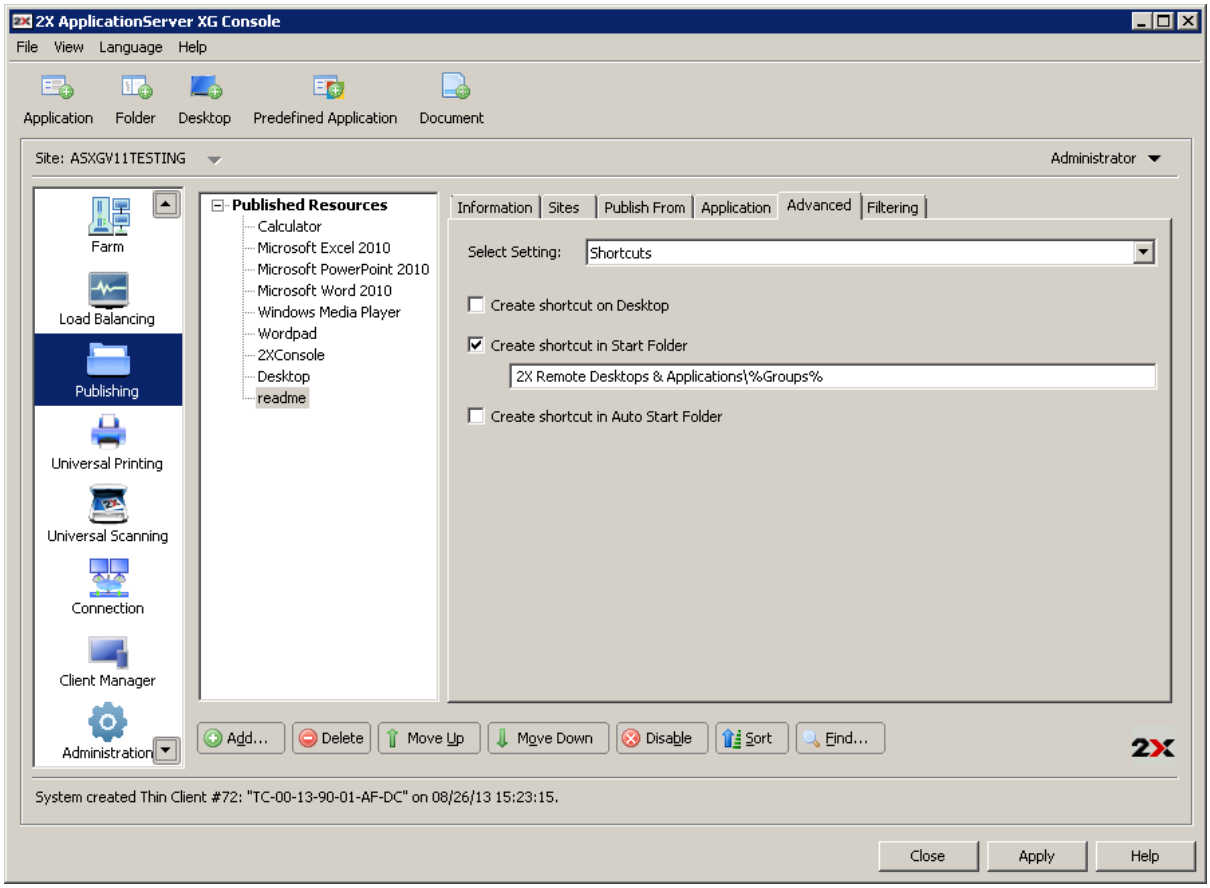
Configuring Server Specific Settings for a Published Document

Configuring Shortcuts Options for a Published Document

.

Click the **Advanced** tab in the application settings and select **Shortcuts** from the **Select Setting** drop down menu to enable the creation of shortcuts on the user's desktop, shortcuts in the start folder with relative folder and shortcut in the Auto start folder. When the Auto start shortcut is enabled the application will be started when the Operating system the client is running is started.

Note: The option is not available on all operating systems.



Configuring the 2X OS Shortcut Options for a Published Document

Managing Published Folders

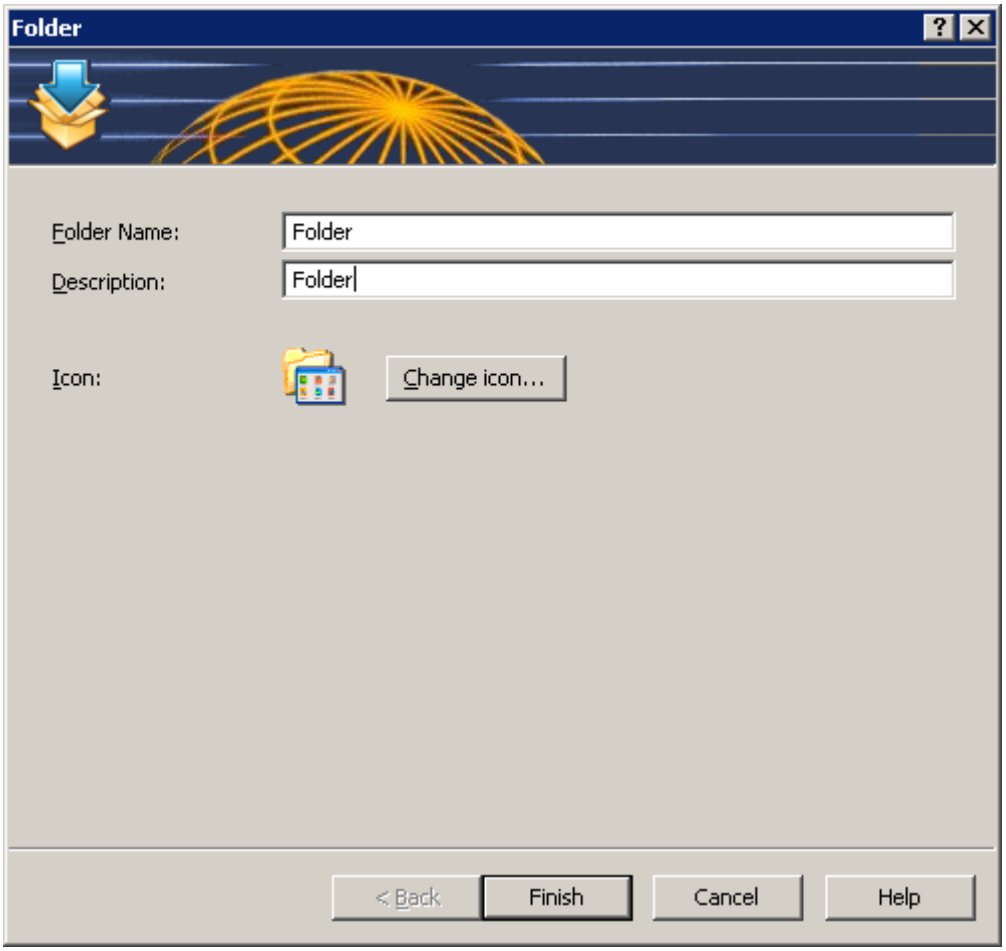
Introduction

Folders can be used to organize published resources and also to facilitate the filtering options. For example you can configure filtering options for a specific folder and then move the published resources under the new folder so the filtering settings are inherited. For more information about Filtering refer to the Filtering section on page 86.

Publishing a Folder

To publish a folder follow the below procedure:

1. Navigate to the **Publishing** category and click the **Folder** icon in the top navigation bar.
2. Specify a folder name in the **Folder** input field and a description in the **Description** input field.
3. (Optional) Change the folder's icon by clicking on the **Change Icon** button.



Publishing a Folder

4. Click **Finish** to publish the folder

Managing Published Folders

Like with any other published resource, you can configure a published folder by selecting its name from the **Published Resources** navigate tree. The below options are available:

Sites Tab

From the sites tab you can specify through which sites the published folder will be available.

Folder Tab

From the folder tab you can configure the folder name and also the description.

Filtering Tab

From the filtering tab you can configure the filtering options for the published folder. The filtering options will be inherited by all other published resources in that folder. For more information about filtering options, refer to the Filtering section on page 86.

Adding Published Resources to a Folder

To add a published resource to a folder select the published resource name and drag it under the folder in the **Published Resources** navigation tree. All published resources in that folder will inherit the folder's filtering options.

Filtering

Introduction

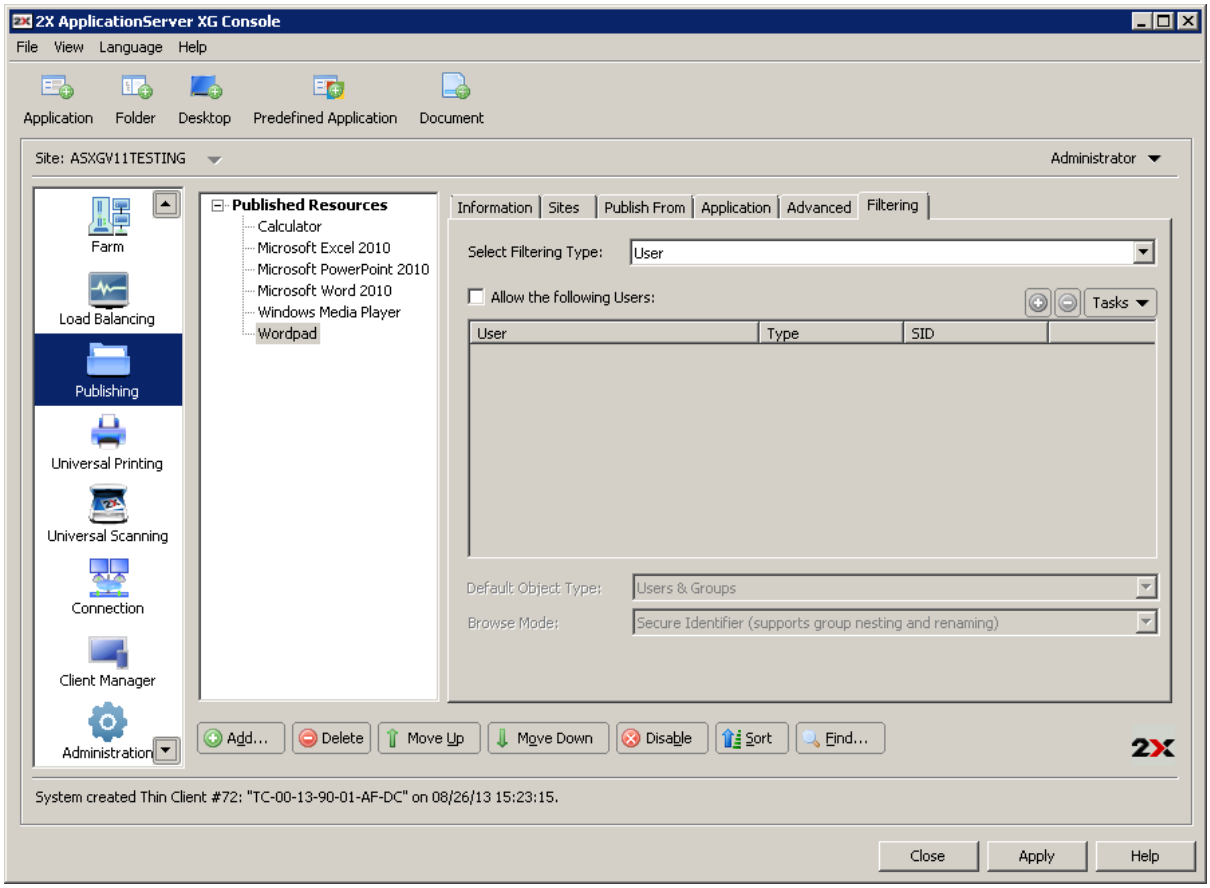
By default there are no filtering rules configured for a published resource, therefore it will be available to anyone who is connected to the 2X ApplicationServer. Filtering allows you to control who can and who cannot access the published resource. You can create several filtering rules based on any of the following filtering options:

- User
- Client (managed client)
- IP Address
- MAC Address
- Gateway

Once you specify a filtering rule, only those who match the rule can access the published resource.

Creating New Filtering Rules

Filtering Rules can be created from the published resource options by selecting the published resource name and click the **Filtering** tab.

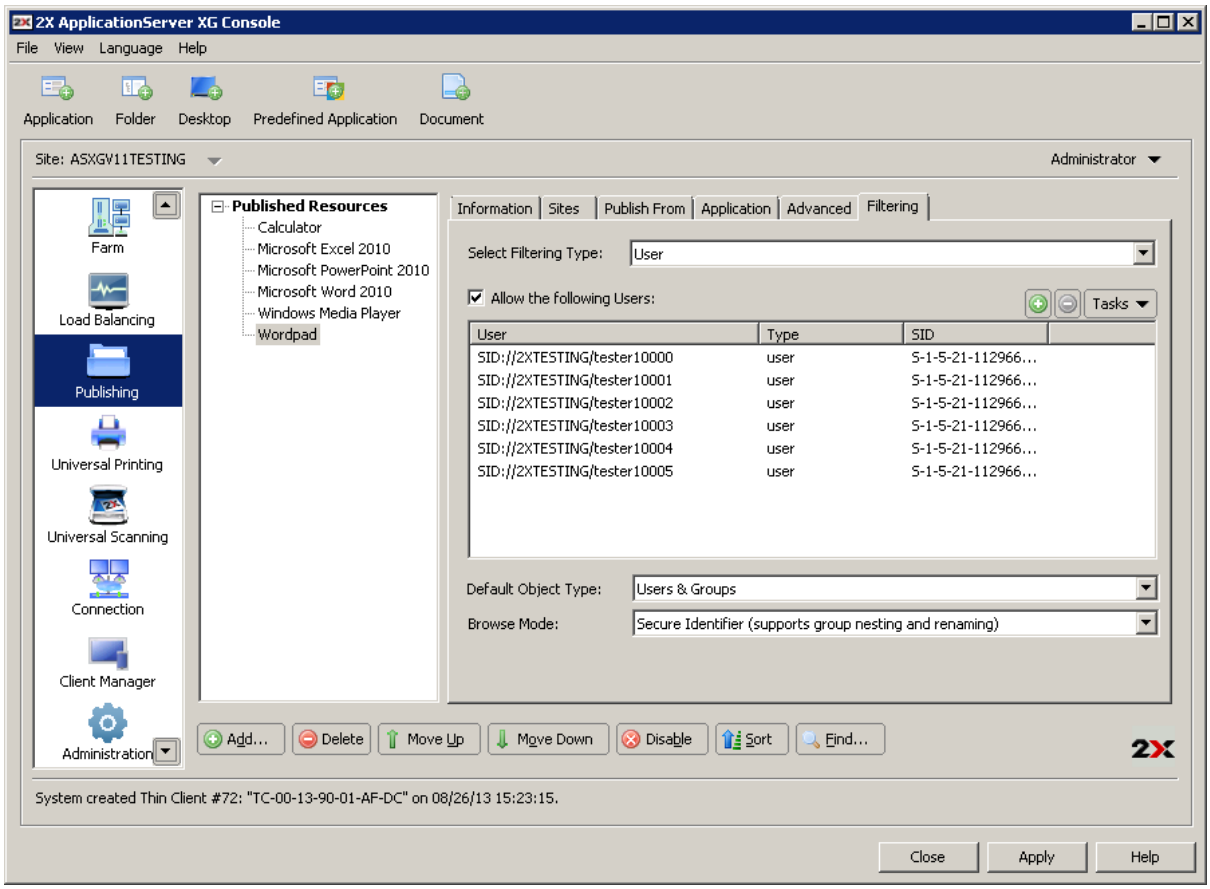


Filtering Options of a Published Resource

Filtering by User

To allow a specific user, list of users or a group to access the published resource, follow the following procedure:

1. Select **User** from the **Search Filtering Type** drop down menu
2. Enable the option **Allow the following Users**
3. Select if you will be specifying users, groups or both from the **Default Object Type** drop down menu.
4. Specify the browsing mode you would like to use to connect to active directory or Windows OS from the **Browse Mode** drop down menu. The options are:
    a. **Secure Identifier**: This is the preferred and fastest method. It supports group nesting and renaming.
    b. **WinNT**: WinNT is faster than LDAP but does not support group nesting. Used only for backward compatibility.
    c. **LDAP**: LDAP supports group nesting but is slow. Used only for backward compatibility.
5. Select **Add** from the **Tasks** drop down menu to specify the user or group from the **Select Users or Groups** dialog box
6. Click **OK** to add the objects to the list.



Configuring User Based Filtering Rules

To delete an object from the list, select the entry from the list and select **Delete** from the **Tasks** drop down menu.

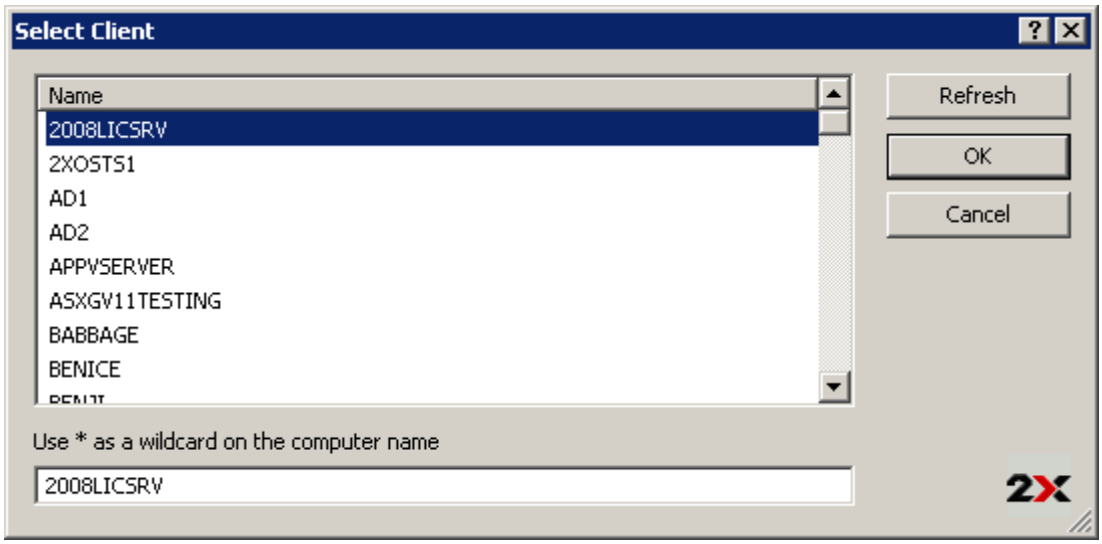
Converting Existing Users to SID

To convert users or groups specified using WinNT or LDAP, select the entry and select **Convert** from the **Tasks** drop down menu.

Filtering by Client

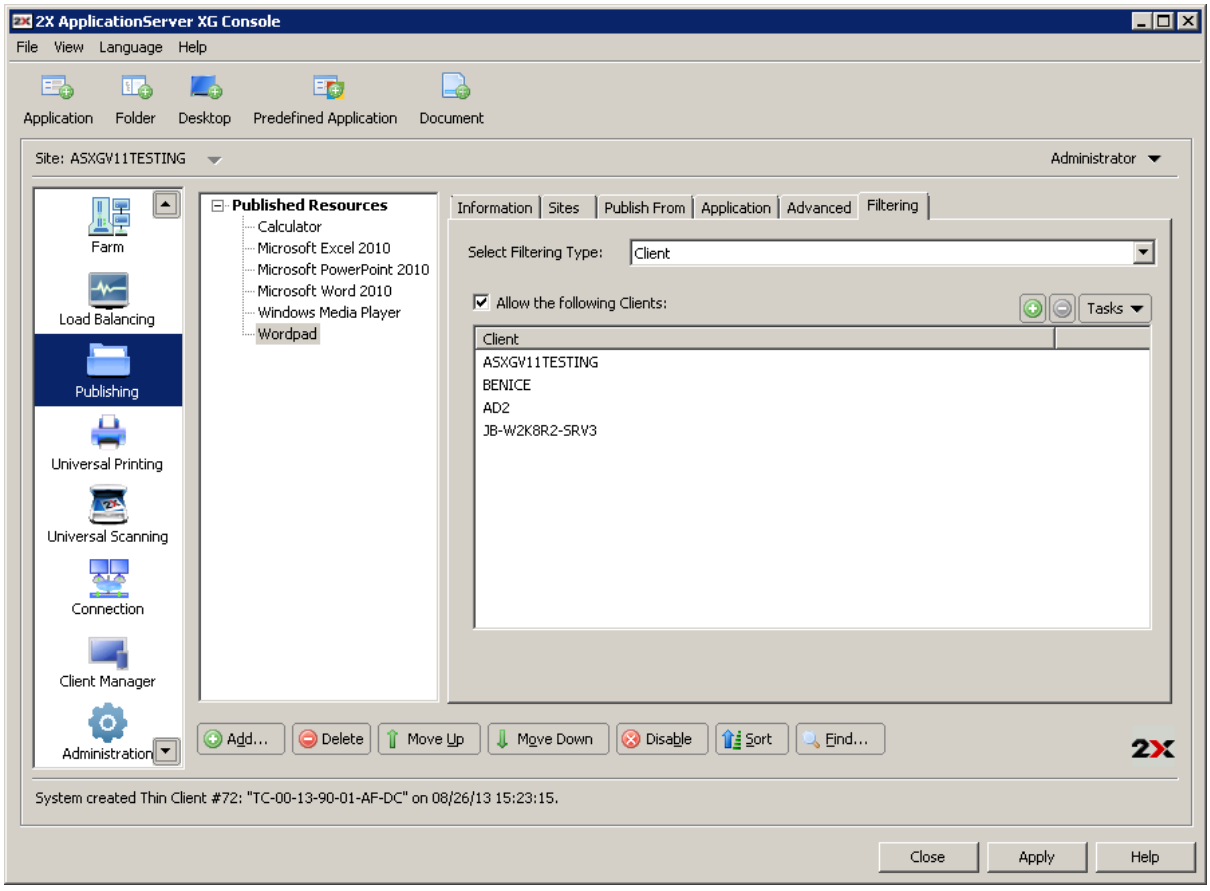
To allow a specific client or a list or clients to access the published resource, follow the following procedure:

1. Select **Client** from the **Search Filtering Type** drop down menu
2. Enable the option **Allow the following Clients**
3. Click **Add** from the **Tasks** drop down menu and select the client(s) from the **Select Client** dialog box



Adding Clients to the Filtering Options

4. Click **OK** to add the clients to the list.



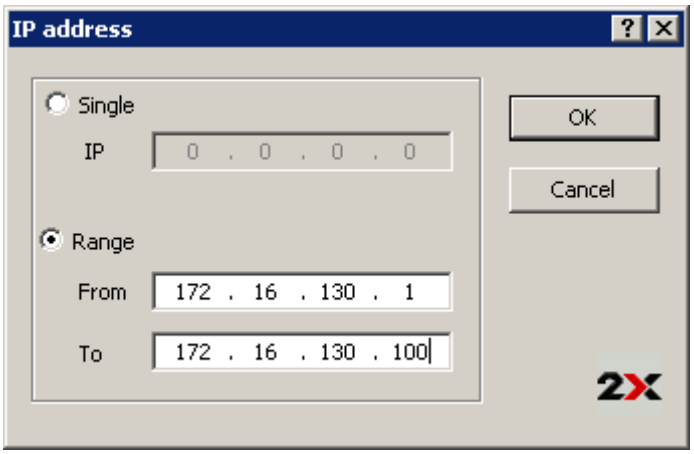
Configuring Client Based Filtering Rules

To delete a client from the list, highlight the entry from the list and click **Delete** from the **Tasks** drop down menu.

Filtering by IP Address

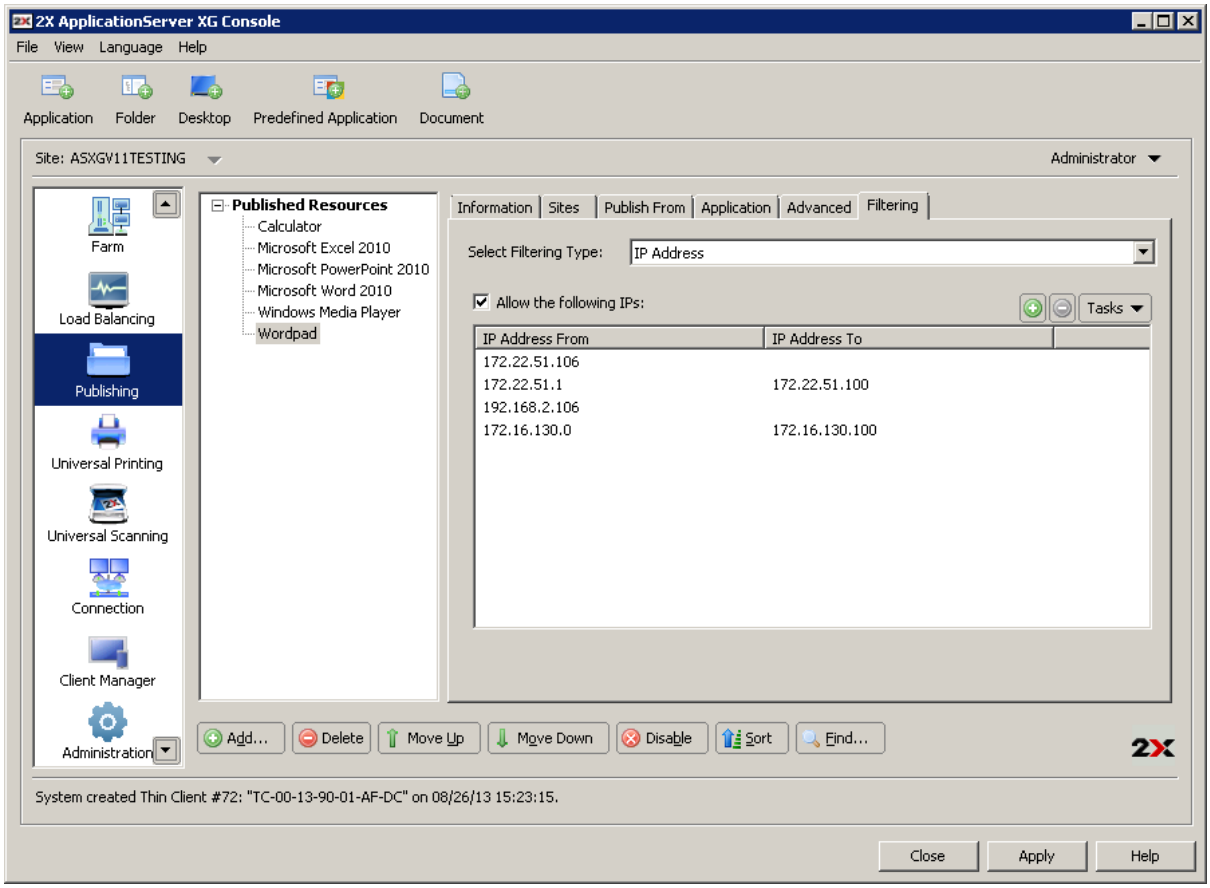
To allow a specific IP or a specific list or range of IP addresses to access the published resource, follow the following procedure:

1. Select **IP Address** from the **Search Filtering Type** drop down menu
2. Enable the option **Allow the following IPs**
3. Click **Add** from the **Tasks** drop down menu to specify the IP Address or a range of IP Addresses and click **OK**



Configuring an IP or Range of IPs for IP Based Filtering Rules

To modify an existing IP range, highlight the entry name from the list and click **Properties**. To delete an IP Address or a range of IP Addresses from the list, highlight the entry from the list and click **Delete** from the **Tasks** drop down menu.

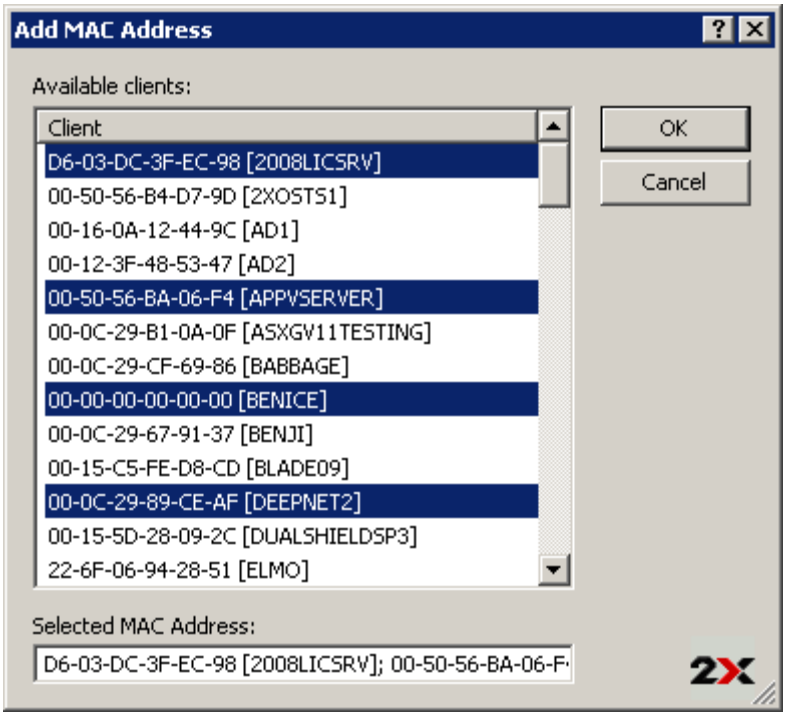


Configuring IP Based Filtering Rules

Filtering by MAC Address

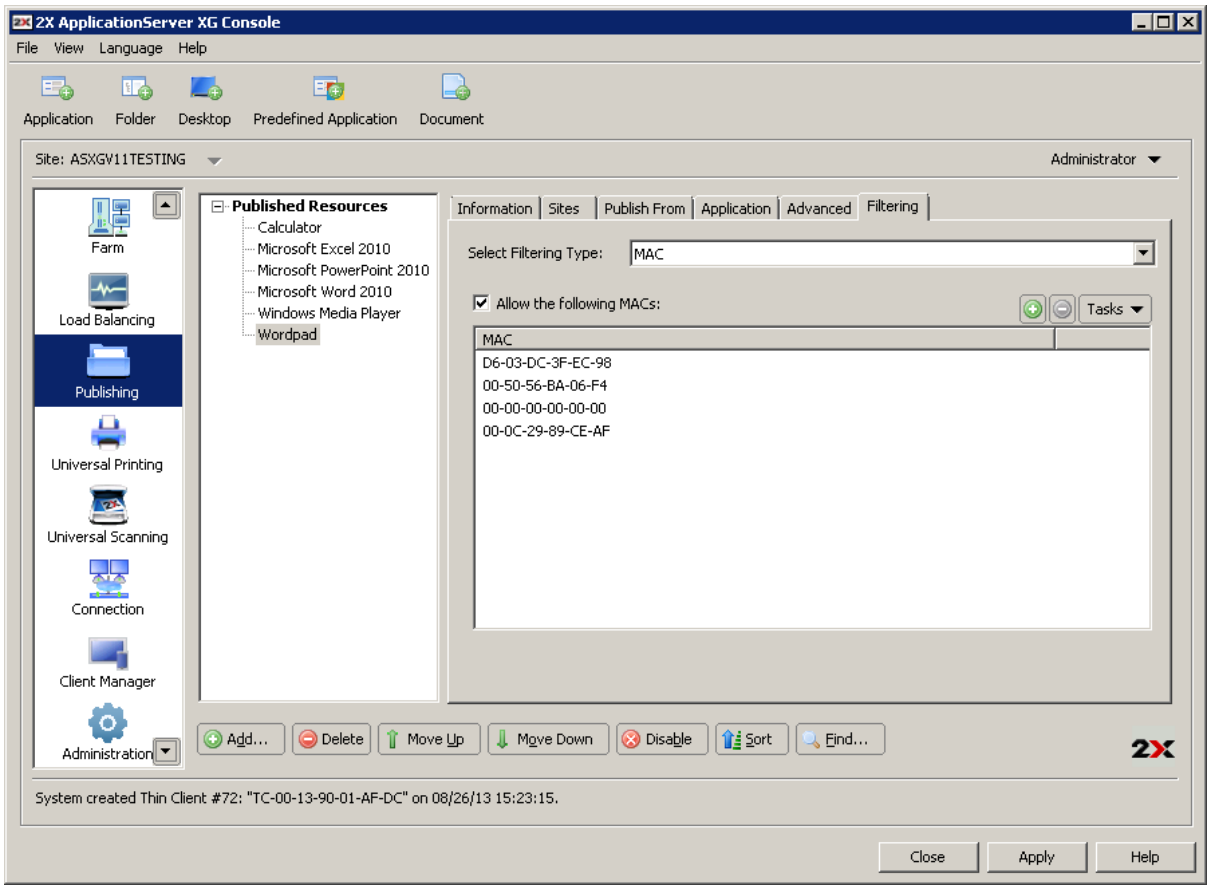
To allow a MAC address or a specific list of MAC addresses to access the published resource, follow the following procedure:

1. Select **MAC** from the **Search Filtering Type** drop down menu
2. Enable the option **Allow the following MACs**
3. Click **Add** from the **Tasks** drop down menu to select the MAC address(es) and click **OK**



Selecting a MAC Address or Addresses MAC Based Filtering Rules

To delete a MAC address from the list, highlight the MAC address from the list and click **Delete** from the **Tasks** drop down menu.

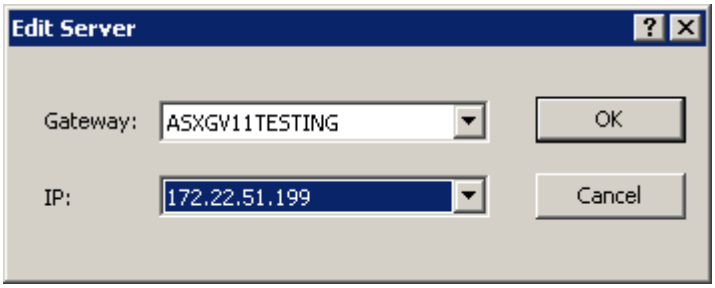


Configuring MAC Based Filtering Rules

Filtering by Gateway

To allow users to connect to a published resource through a specific gateway only, follow the following procedure:

4. Select **Gateway** from the **Search Filtering Type** drop down menu
5. Enable the option **Allow connects through these Gateways**
6. Click **Add** from the **Tasks** drop down menu to specify the Gateway and its IP address, if it has multiple IP addresses



Configuring a Gateway and its IP for Gateway Based Filtering Rules

To delete a Gateway from the list highlight the entry from the list and click **Delete** from the **Tasks** drop down menu.

Configuring Multiple Filtering Rules

If multiple filtering rules are configured for a specific published resource, the connecting user has to match ALL the configured filtering rules to be allowed access to the published resource.

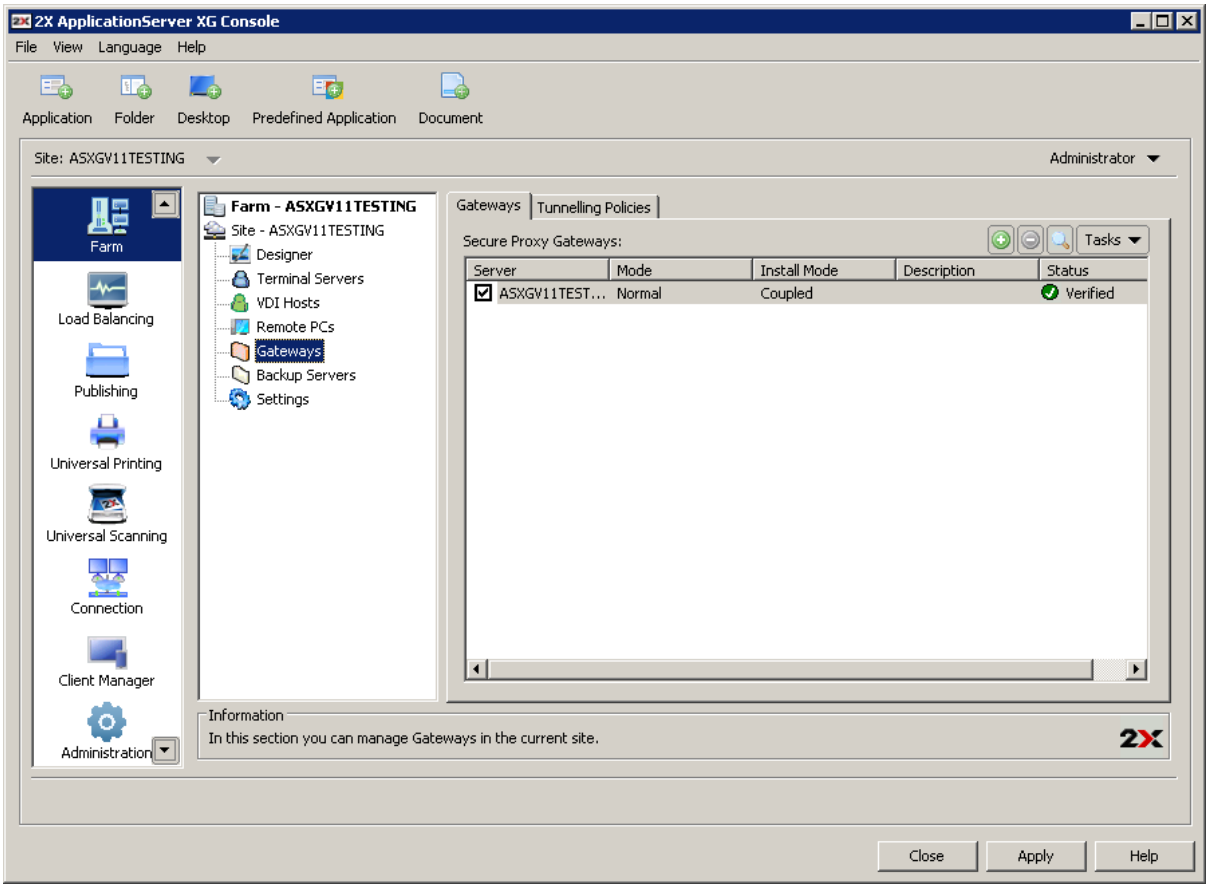
For example if you configure a user filter rule for user **admin** and another MAC address filter rule for MAC address **AB-CD-12-34-A1-C2**, unless the user **admin** accesses the published resource from a client with the MAC address **AB-CD-12-34-A1-C2**, the user won't be allowed access to the published resource.

2X Secure Client Gateways

Introduction

The 2X Secure Client Gateway tunnels all the 2X ApplicationServer XG data on a single port. It also provides secure connections and is the user connection point to the 2X ApplicationServer XG.

By default the 2X Secure Client Gateway is installed on the same server where the 2X ApplicationServer XG is installed. You can add additional 2X Secure Client Gateways in a site to support more users, load balance connections and provide redundancy.



Accessing List of Gateways in a Site

How a Gateway Works

The use of the 2X Secure Client Gateway in the 2X ApplicationServer XG site is explained below:

1. Gateway receives a user connection request.

2. Gateway forwards the request to all the Publishing Agents in the farm.
3. Publishing Agent performs Load Balancing checks and Active Directory security lookup to obtain security permissions.
4. If the user requesting a published resource is granted, the publishing agent returns the response to the gateway service including details about which terminal server the user can connect to.
5. Depending on the connection mode, the client either connects through the gateway or disconnects from the gateway and connects directly to the RDS Server.

2X Secure Client Gateway Types

Normal Mode

A gateway in normal mode will receive user connection requests and checks with the Publishing Agent if the user making the request has access or not. Normal gateways can be used to support a larger number of requests and to improve redundancy.

Forward Mode

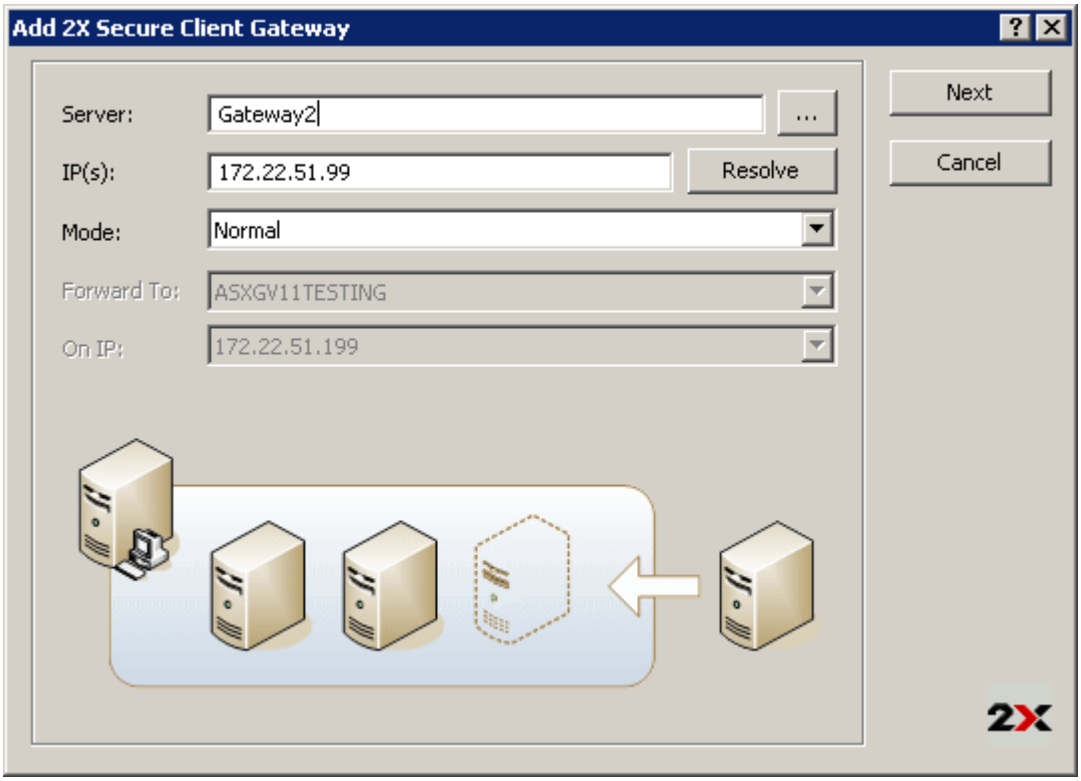
A gateway in forwarding mode will forward all the user connection requests to a pre configured gateway. Gateways in forward mode are useful if cascading firewalls are in use, to separate WAN connections from LAN connections and make it possible to disconnect WAN segments in the event of issues without disrupting the LAN.

Note: Multiple Gateways are needed to configure a gateway in Forward mode.

Adding a 2X Secure Client Gateway

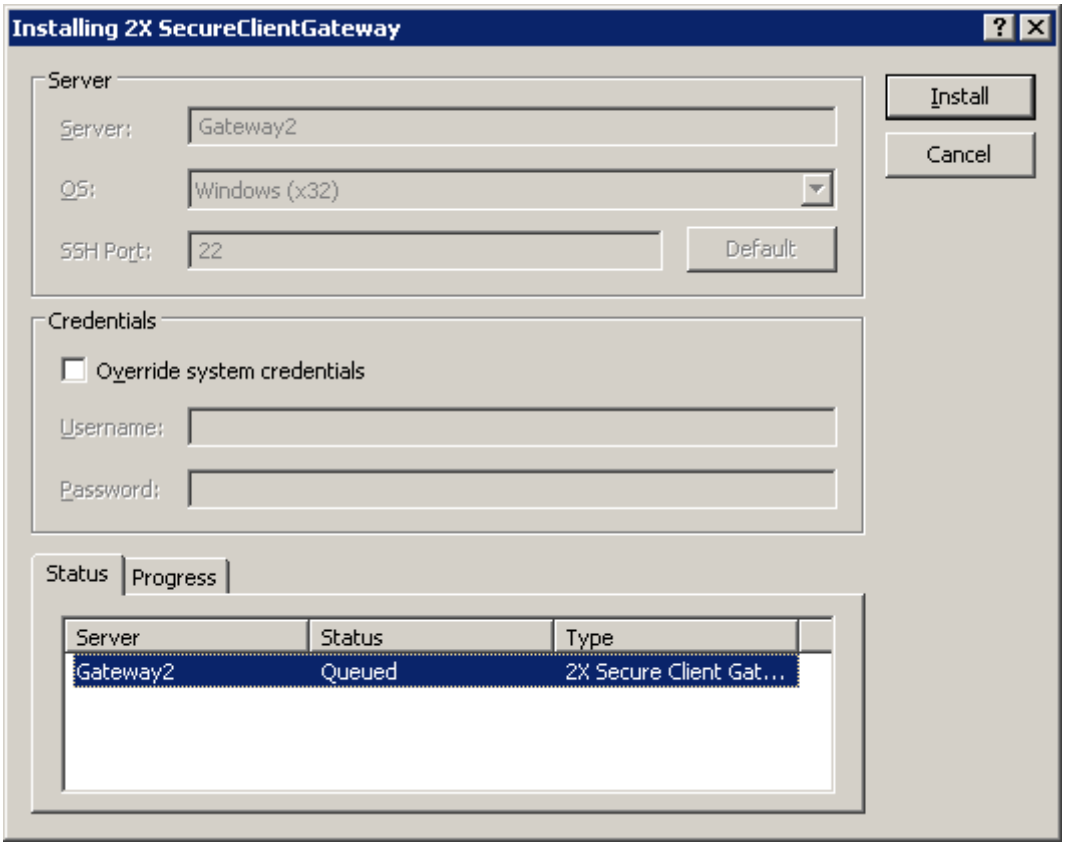
To add a 2X Secure Client Gateway to a site follow the below procedure:

1. Open the 2X ApplicationServer Console and select the **Gateway** node from the navigation tree.
2. Click **Install** from the **Tasks** drop down menu to launch the Add 2X Secure Client Gateway wizard.
3. In the first step of the wizard enter the server **FQDN** or **IP** or click the **Browse** button to select a server from the list.
4. Select the gateway mode from the **Mode** drop down menu.
5. If you select **Forwarding** mode specify the gateway where the traffic should be forwarded to from the **Forward To** drop down menu and click **Next**.



Adding a New Gateway

6. In the second step you have to remotely install the 2X SecureClientGateway service on the target machine. Highlight the server name and tick the option **Override system credentials** to specify different credentials to access the server using a different set of credentials.



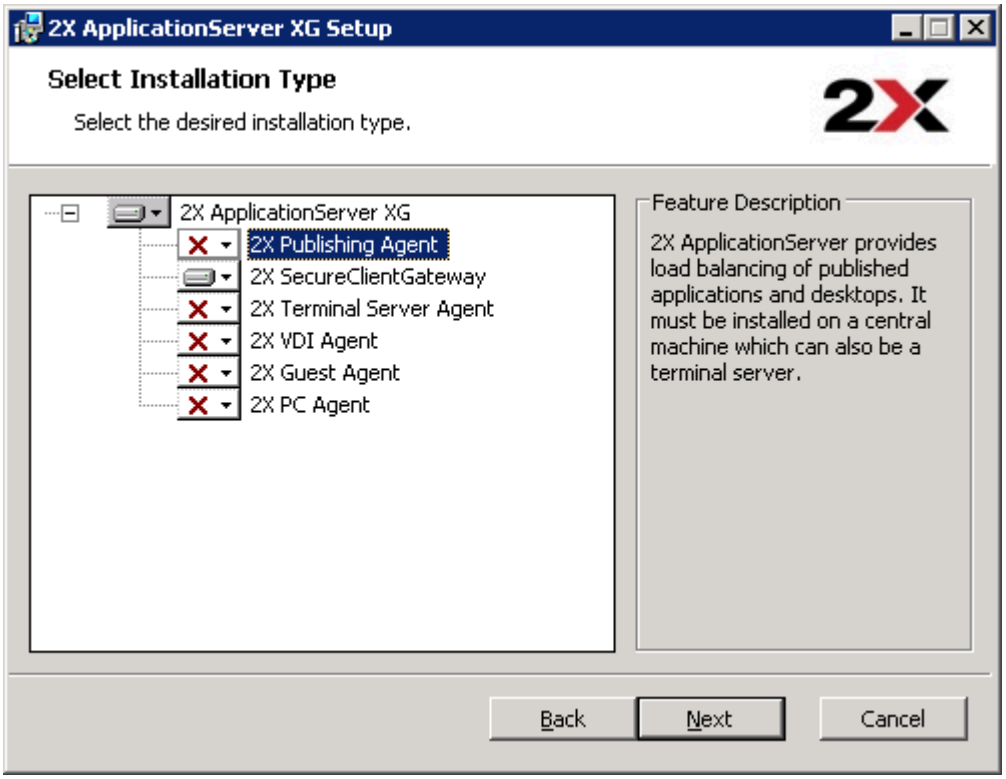
Installing the 2X SecureClientGateway Service

7. Click **Install** to start the 2X SecureClientGateway Installation and **Done** once the installation is ready.

Manually Adding a 2X Secure Client Gateway

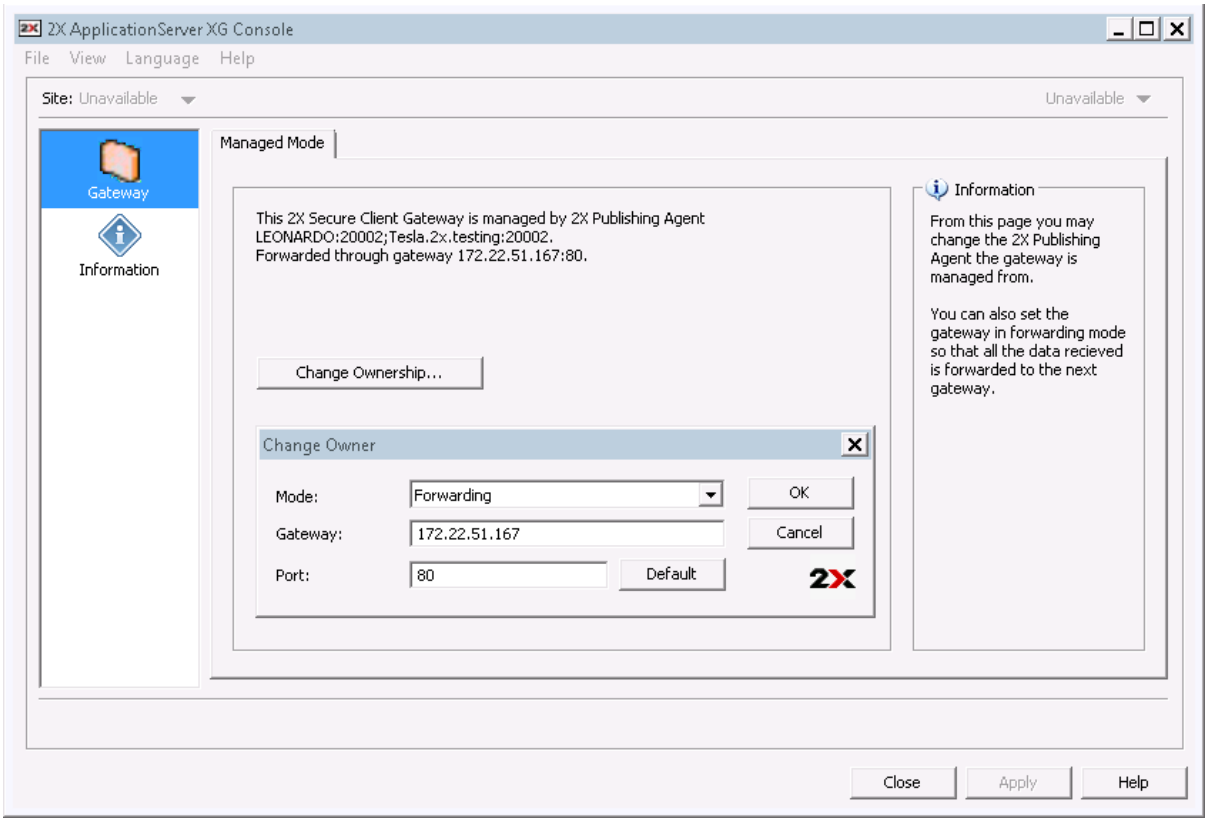
To manually install a 2X Secure Client Gateway and add it to the farm, follow the below procedure:

1. Login to the server where you will be installing the 2X Agent using an administrator account and close all other applications.
2. Copy the 2X ApplicationServer XG installation file (**2XAppServer.msi**) to the server and double click it to launch the installation.
3. Once prompted click **Next** and accept the End-User license agreement.
4. Select the path where the 2X Secure Client Gateway should be installed and click **Next**.
5. Select **Custom** from the installation type screen and click **Next**.
6. Click on **2X SecureClientGateway** in the feature tree and select **Entire Feature will be installed on local hard drive to** install it as seen in the below screenshot.


2X ApplicationServer XG Setup
Select Installation Type
Select the desired installation type.
2X ApplicationServer XG
2X Publishing Agent
2X SecureClientGateway
2X Terminal Server Agent
2X VDI Agent
2X Guest Agent
2X PC Agent
Feature Description
2X ApplicationServer provides load balancing of published applications and desktops. It must be installed on a central machine which can also be a terminal server.
Back
Next
Cancel

Manually Installing the 2X SecureClientGateway

7. Ensure that all other components in the selection tree are deselected and click **Next**.
8. Click **Install** to start the installation and **Finish** once the installation is ready to close the wizard.
9. After the installation is done, the administrator needs to deploy the console and configure where the 2X Publishing agent is, as seen in the below screenshot.



Manually Configuring the 2X SecureClientGateway

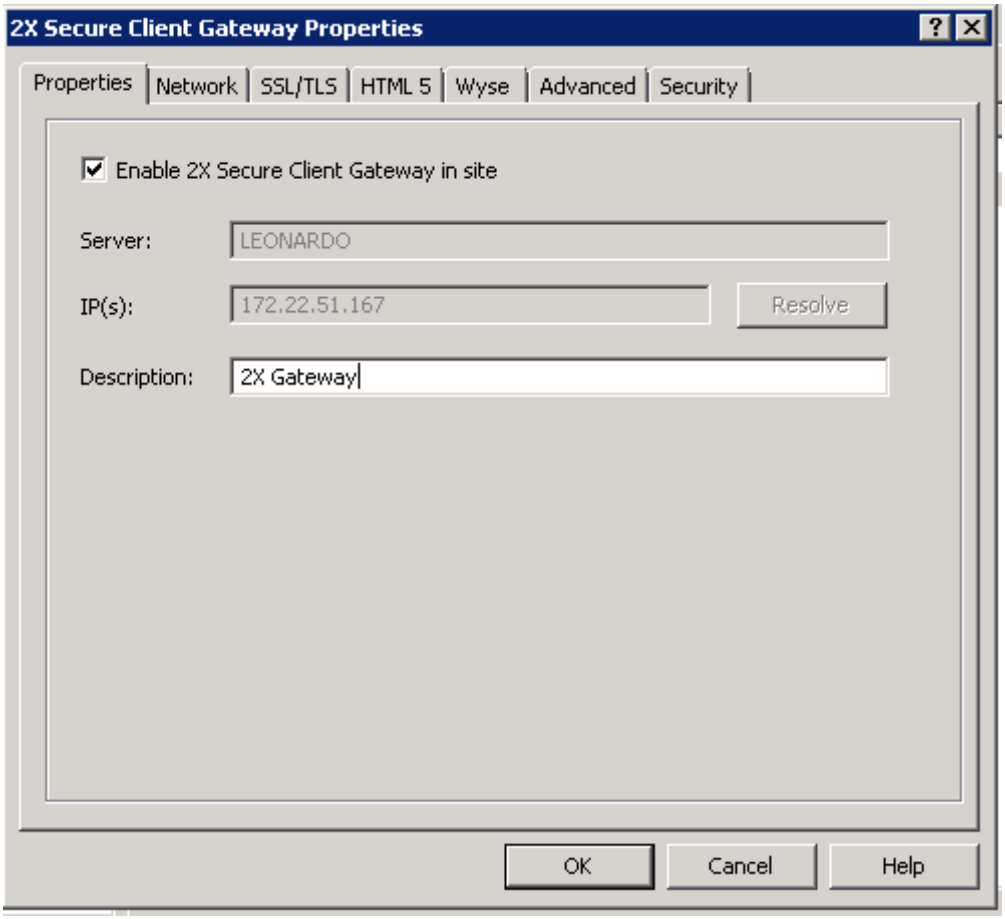
Managing 2X Secure Client Gateways

Introduction

To access a Gateway options, highlight the gateway from the **Gateways** node and click **Properties** from the **Tasks** drop down menu.

Enabling and Disabling a Gateway

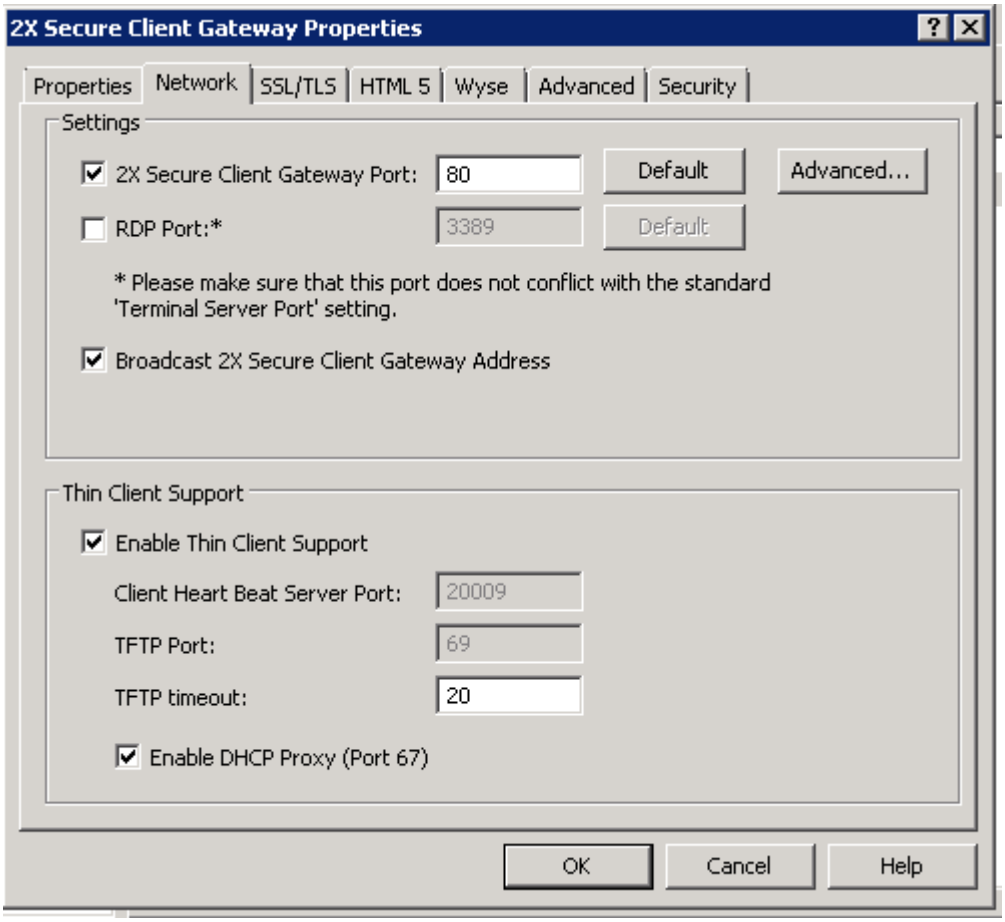
By default a Gateway is enabled in the site. To disable a Gateway untick the option **Enable 2X Secure Client Gateway in farm** from the **Properties** tab.



Enabling or Disabling a Gateway in the site

Configuring the 2X Secure Client Gateway Port

By default the gateway listens on TCP port 80 to tunnel all the 2X ApplicationServer XG traffic. To change the port, select the **Network** tab and specify a new port in the **2X Secure Client Gateway Port** input field.



Configuring Gateway Ports and Thin Client Support

RDP Port

Port TCP 3389 is used with the 2X Load Balancer for clients who require basic load balanced desktop sessions. Connections on this port do **NOT** support published items.

To change the RDP port on a gateway select the **Network** tab, tick the **RDP Port** option and specify a new port.

Note: If this port is changed the users need to append the port number to their connection string in the remote desktop client (e.g. [ip address]:[port]).

Configuring Thin Client and 2XOS Support

Note: Only gateways in normal mode support Thin Clients and network booting.

To configure a gateway to manage thin clients, and to allow them to network boot using the 2XOS tick the option **Enable Thin Client Support** from the **Network** tab in the gateway properties as show in the above screenshot. From this section you can also configure the following options:

- **TFTP Timeout**: Default value is of 20 seconds. If you are experiencing timeouts increase this value.
- **Enable DHCP Proxy**: If this option is enabled, the gateway will listen on Port 67 for thin client broadcasts and on receipt, it will deliver the configured 2XOS build to the thin client.

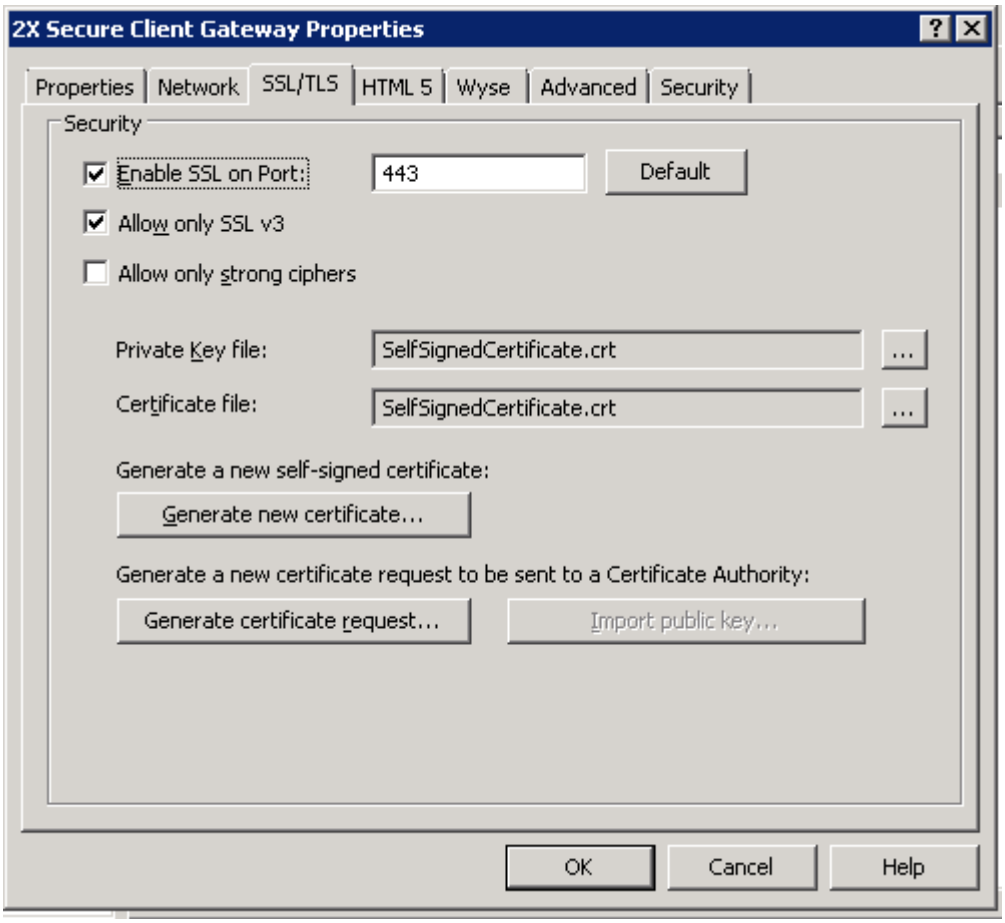
Enabling SSL Encryption on 2X Secure Client Gateway

The traffic between the users and the gateway is always encrypted. To enable the HTML 5 Gateway and also encrypt the HTTP traffic when the gateway is enabled using a self-signed certificate follow the below procedure:

1. Navigate to the **SSL/TLS** tab in the gateway properties.
2. Tick the option **Enable SSL on Port** and configure a port number (default is 443).
3. (Optional) Tick the option **Allow Only SSL v3** to only allow SSL v3 connections. By default the 2X Secure Client Gateway supports both version 2 and version 3 SSL.
4. (Optional) Tick the option **Allow only strong ciphers** to only allow the usage of certificates using strong encryption algorithms.
5. Click on **Generate new certificate** and enter the required details.

Note: To enable SSL using a certificate from a trusted authority, follow the procedure 'Use a Certificate from a Trusted Authority for SSL'.

6. Click **Save** to save all the details and generate a new self-signed certificate. The **private key file** and **Certificate file** will be automatically populated.
7. Click **OK** to save the options.



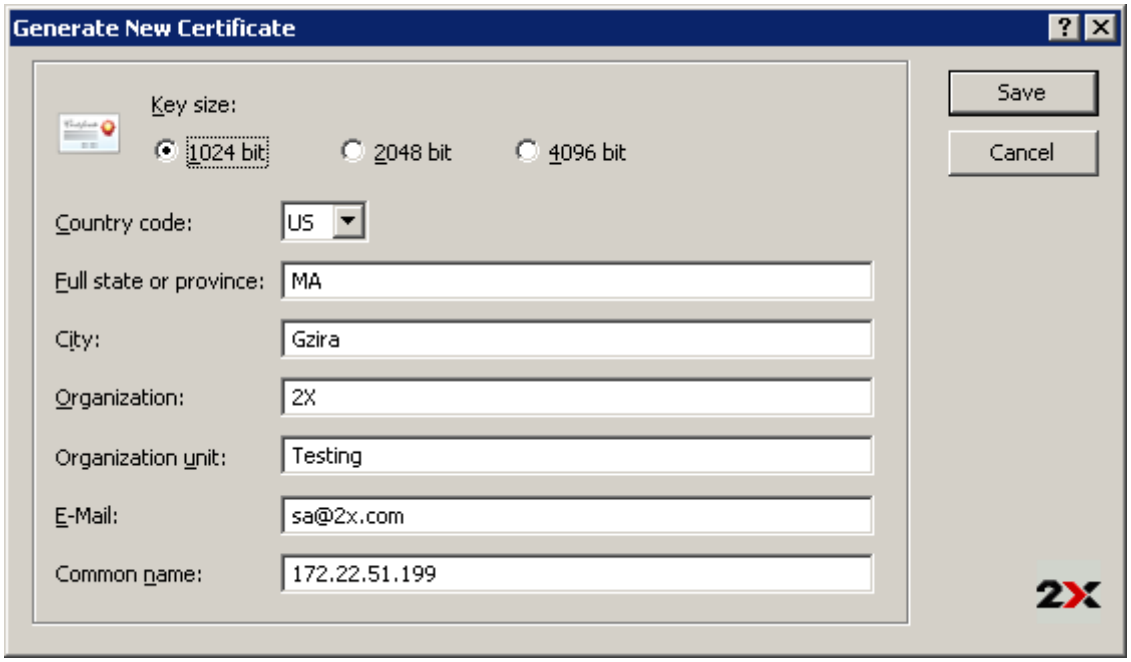
Enabling SSL/TLS Support on a Gateway

Note: By default only the connection between the gateway and the servers is encrypted. Change the connection mode to **Gateway SSL Mode** from the connection properties on all 2X clients to also encrypt the connection between the users and the gateway.

Use a Certificate from a Trusted Authority for SSL

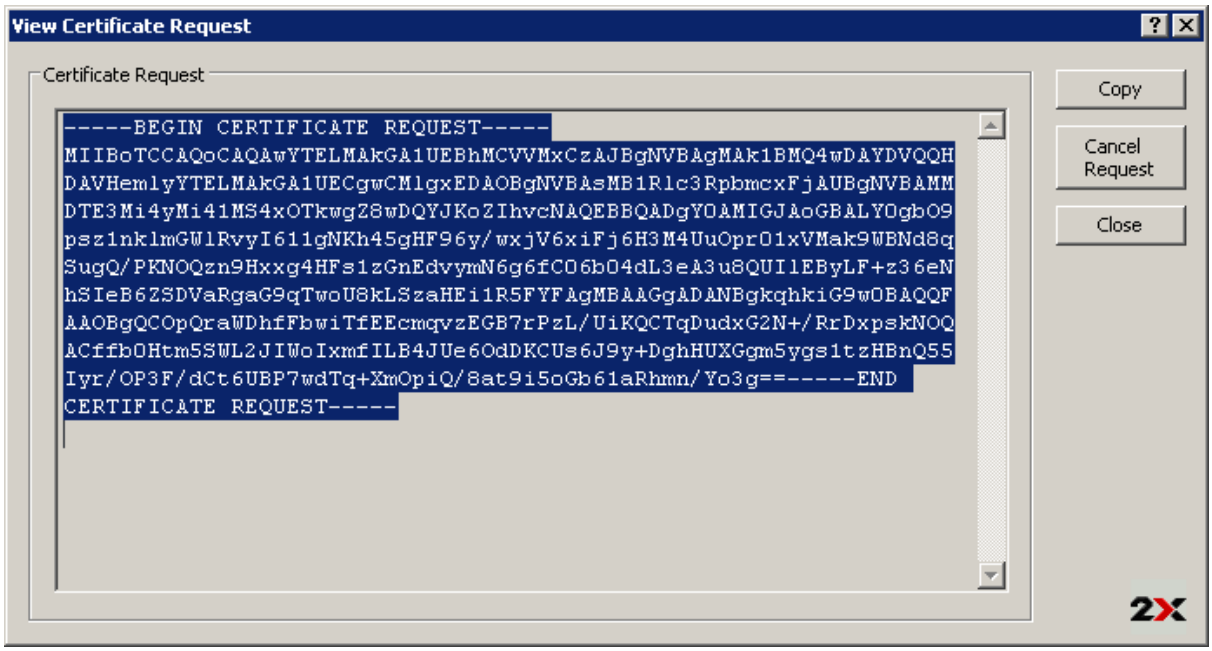
To use a certificate from a trusted authority to enable SSL on a 2X Secure Client Gateway, follow the instruction below:

1. Navigate to the **SSL/TLS** tab in the gateway properties.
2. Click on **Generate certificate request**, fill in all the required details and click **Save**.



Configuring SSL Certificate Details

3. Once ready a window will pop up with the certificate request, as show in the below screenshot. Click **Copy** to copy the request which you should send to the certificate authority.



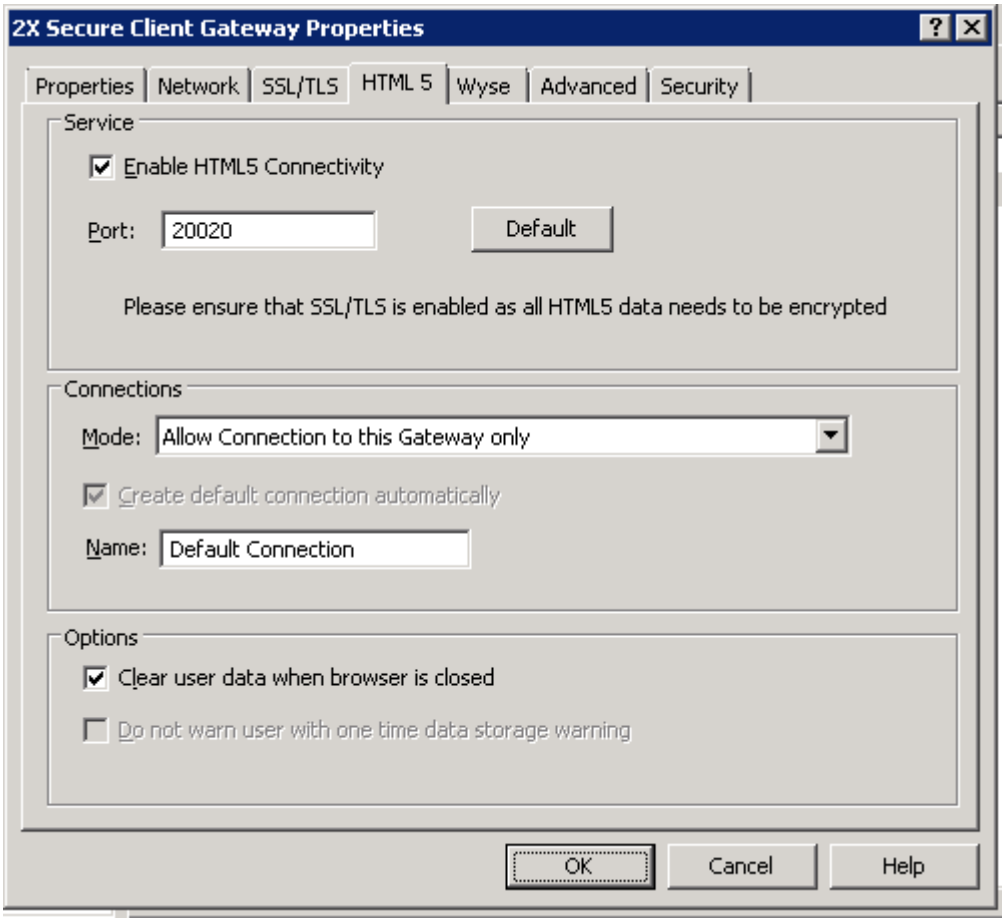
Generated Certificate Request

4. Once you receive the SSL certificate from the certificate authority click on **Import public key**, browse for the certificate file containing the public key and click **Open**.
5. Click **OK** to save the settings.

Enabling HTML 5 Support on the Gateway

Requirement: To enable HTML 5 support on a gateway, SSL/TLS should be enabled and configured.

To enable HTML 5 support on a gateway, tick the option **Enable HTML 5 Connectivity** from the **Services** section in the **HTML 5** tab. From the same section you can also configure the **Port** which the gateway uses to connect to the HTML 5 module.



Configuring HTML 5 Options on a Gateway

Configuring HTML 5 Connection User Capabilities

From the **Connections** section in the **HTML 5** tab you can configure what capabilities a user have when connected to the HTML 5 session. The options that can be configured from the **Mode** drop down menu are:

Allow Connection to this Gateway Only

Select this option so users can only access a connection to this gateway from the HTML 5 interface. Tick the option **Create Default Connection** so the connection to the gateway is already available in the HTML 5 interface.

Allow Modification of 2X Connections

Select this option to allow users to create new connections to other gateways or modify existing ones from the HTML 5 interface.

Allow Modification of 2X and RDP Connections

Select this option to allow users to create new connections to other gateways or modify existing ones, and also allow them to create new RDP connections from the HTML 5 interface.

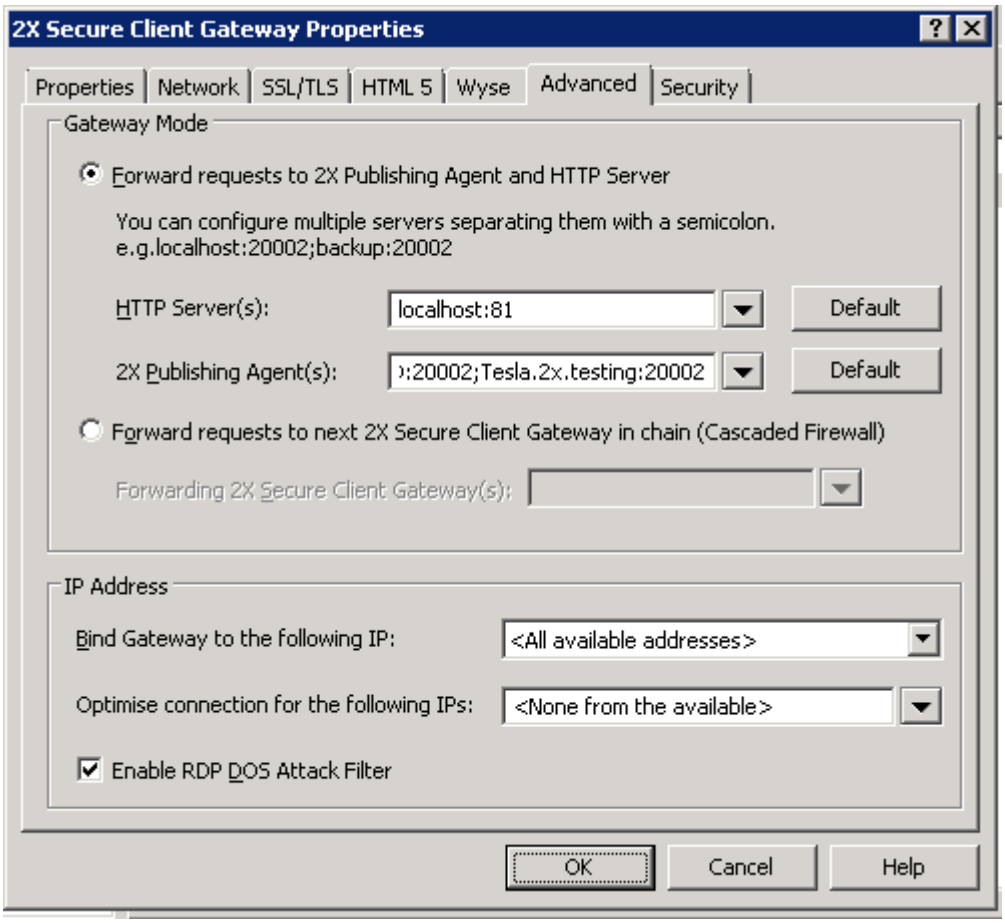
Accessing the HTML 5 Interface

To connect to the HTML 5 interface of a gateway and access published resources, use an HTML 5 capable browser and connect to the following URL:

https://[Hostname]/2XHTML5Gateway/

Changing the Gateway Mode and Forwarding Settings

To change the gateway mode from normal to forwarding mode or vice versa and configure related settings select the **Advanced** tab from the gateway properties.



Configuring Gateway Advanced Options

Normal Mode

Select **Forward requests to 2X Publishing Agent and HTTP Server** to set the gateway to normal mode.

From this tab you can also configure the HTTP server and 2X Publishing Agent the gateway forwards requests to from the **HTTP Server(s)** and **2X Publishing Agent(s)** drop down menus.

Forwarding Mode

Select **Forward requests to next 2X Secure Client Gateway in chain (cascaded Firewall)** to set the gateway to forwarding mode.

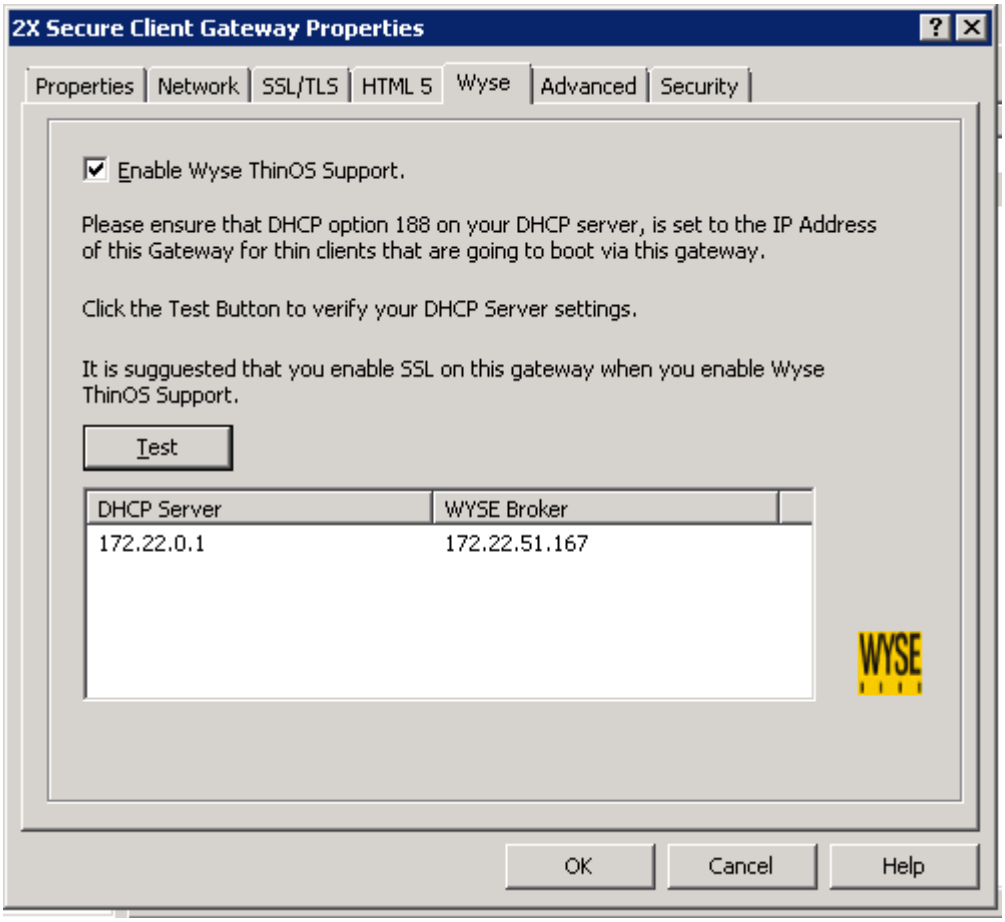
Select the forwarding gateway from the **Forwarding 2X Secure Client Gateway(s)** drop down menu.

Managing Multiple IP Addresses on a Gateway

If the gateway has multiple addresses you can configure the gateway to listen and optimise the connection on a single IP address from the **IP Address** section in the **Advanced** tab shown in the above screenshot.

Support for Wyse Thin Client OS

To publish applications from the 2X ApplicationServer XG to Thin Clients using the Wyse ThinClient OS, tick the option **Enable Wyse ThinOS Support** from the **Wyse** tab in the gateway properties.


2X Secure Client Gateway Properties
Properties
Network
SSL/TLS
HTML 5
Wyse
Advanced
Security
Enable Wyse ThinOS Support.
Please ensure that DHCP option 188 on your DHCP server, is set to the IP Address of this Gateway for thin clients that are going to boot via this gateway.
Click the Test Button to verify your DHCP Server settings.
It is sugguested that you enable SSL on this gateway when you enable Wyse ThinOS Support.
Test
DHCP Server
WYSE Broker
172.22.0.1
172.22.51.167
WYSE
OK
Cancel
Help

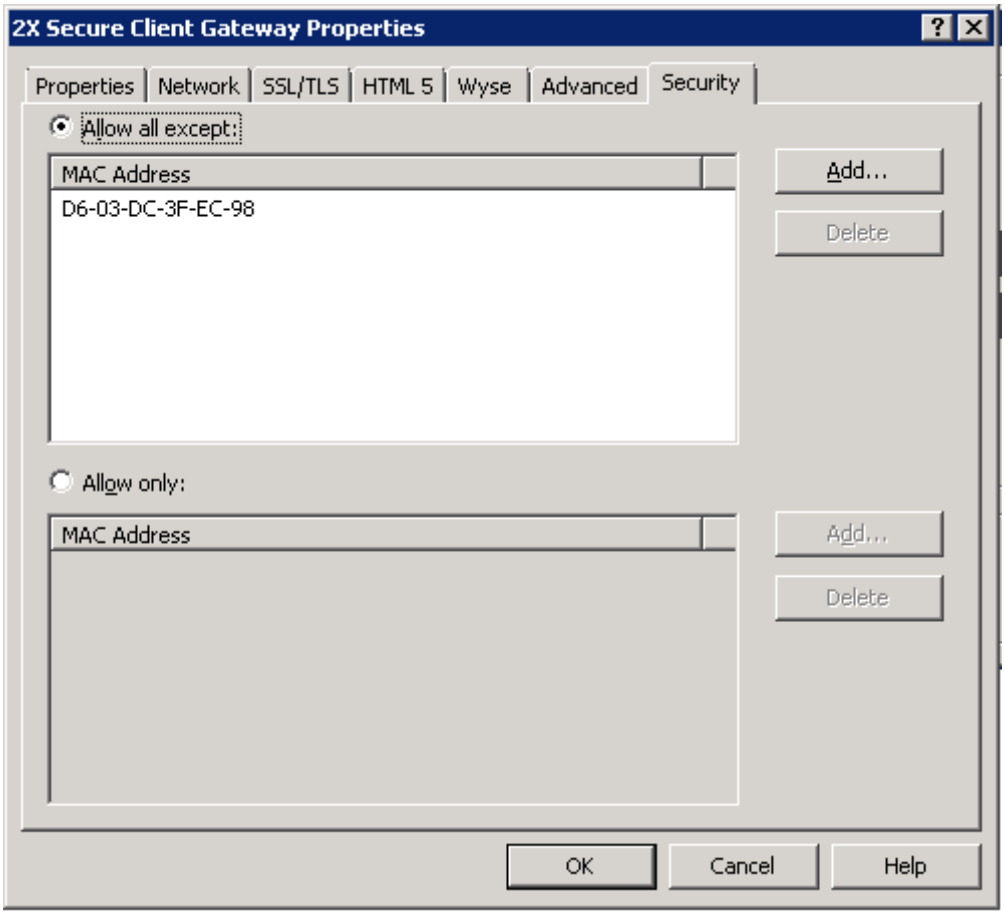
Configuring a Gateway to Support WYSE Thin Client OS

By enabling this option, the 2X Secure Client Gateway will act as a Wyse broker. Once the DHCP server is configured as explained in the tab, click the **Test** button to verify the DHCP server settings.

Filtering Access to 2X Secure Client Gateway

You can allow or deny users from accessing a gateway based on MAC addresses. To configure a list of allowed or denied MAC addresses navigate to the **Security** tab in the gateway properties. The options are:

- **Allow all except**: if this option is enabled then all devices on the network will be allowed to connect to the gateway apart from those listed in this list.
- **Allow only**: if this option is enabled only the list of MAC addresses in the list are allowed to connect to the gateway.



Restricting Access to a Gateway via MAC Addresses

Miscellaneous Gateway Settings

Broadcast Gateway Address

The option **Broadcast 2X Secure Client Gateway Address** in the gateway properties **Network** tab can be used to switch on the broadcasting of the gateway address so 2X clients can automatically find their primary gateway.

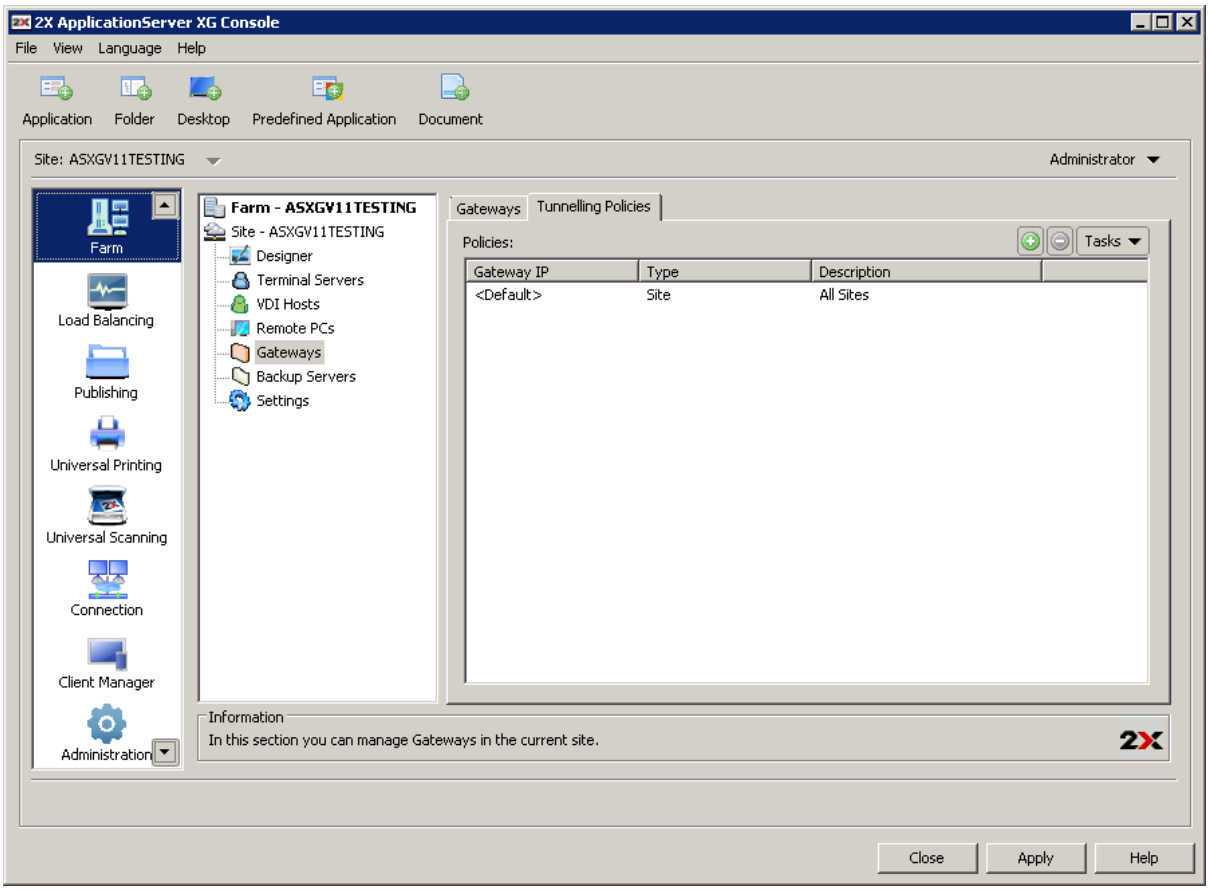
Configuring Listening IP Address

If the server the 2X Secure Client Gateway is running on has multiple IP addresses, by default the gateway will listen on all IP addresses. To configure the gateway to listen on a specific IP address, select the IP address form the **Bind Gateway to the following IP** drop down menu which can be found in the **Advanced** tab in the gateway properties.

Gateway Tunnelling Policies

Introduction

Tunnelling policies can be used to load balance connections by assigning a group of terminal servers to a specific 2X Secure Client Gateway or 2X Secure Client Gateway IP. Tunnelling Policies can be configured from the **Tunnelling Policies** tab in the **Gateways** node. These policies are used when a native RDP connection is established to the gateway.



Configuring Tunnelling Policies

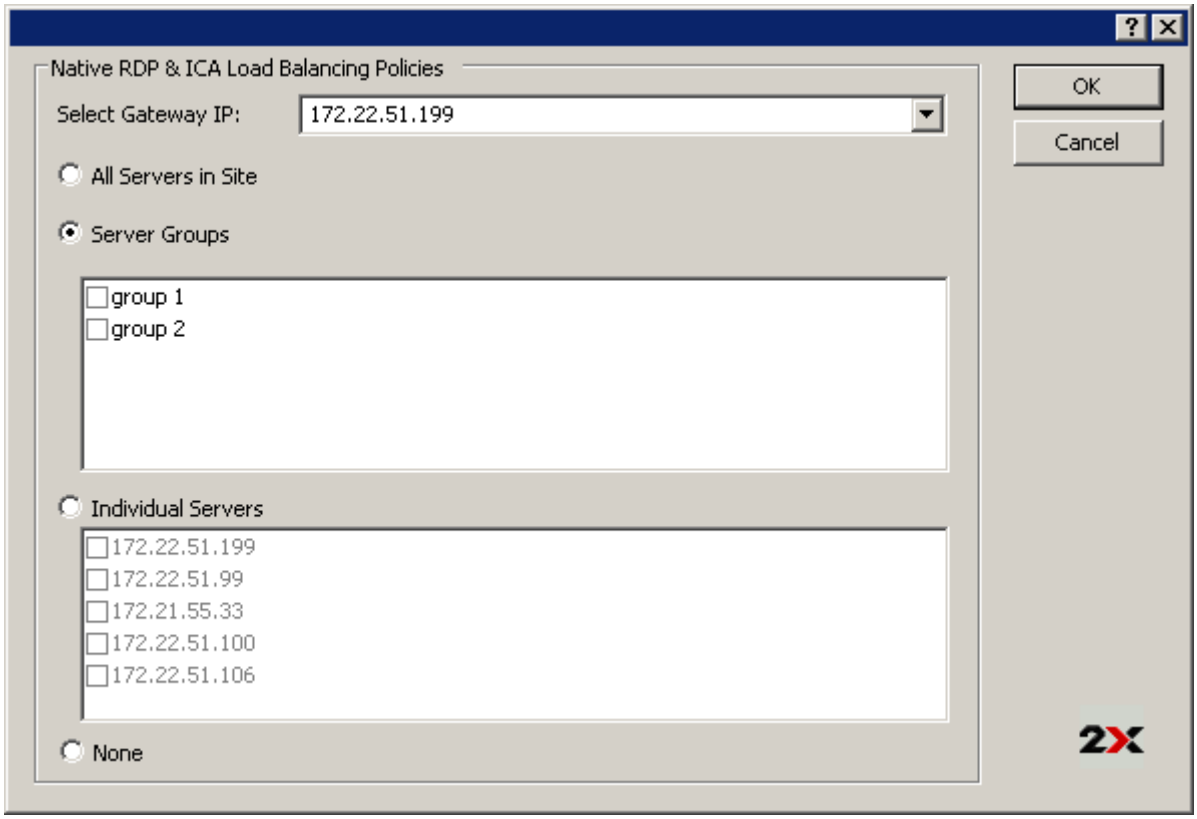
Configuring Tunnelling Policies

The **<Default>** rule is a pre-configured rule and is always the last rule to catch all non configured gateway IPs and load balance the sessions between all servers in the farm. You can configure the **<Default>** rule by clicking **Properties** from the **Tunnelling Policies** tab.

Adding a New Tunnelling Policy

To add a new rule follow the below procedure:

1. Click **Add** from the **Tasks** drop down menu.
2. Select a Gateway IP from the **Select Gateway IP** drop down menu.
3. Specify to which Terminal Server or Servers the users connecting to that specific Gateway IP should be forwarded to. The options are to all servers, group of servers or an individual, or group of individual servers.



Configuring a New Tunnelling Policy

Managing Tunnelling Policies

To modify an existing Tunnelling Policy highlight the policy name and click **Properties** from the **Tasks** drop down menu. To delete a Tunnelling Policy, highlight the policy name and click **Delete** from the **Tasks** drop down menu.

2X Backup Servers

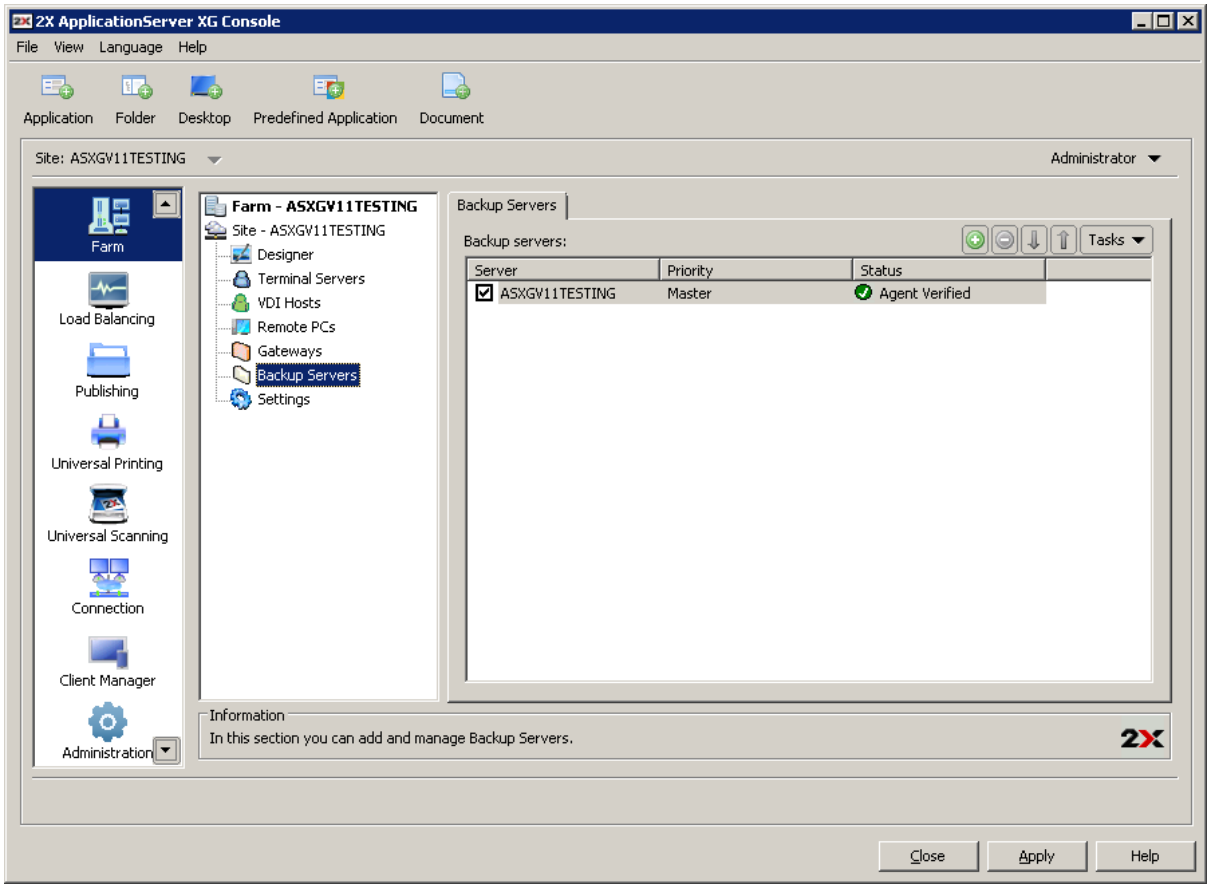
Introduction

To ensure users do not experience any interruption of the service due to a failure of the primary 2X Publishing Agent, a backup Publishing Agent server can be configured for each site in the 2X ApplicationServer XG farm.

Adding a 2X Backup Server

To add a backup server to a site follow the procedure below:

1. Open the 2X ApplicationServer console and navigate to the **Backup Servers** node in the navigation tree.



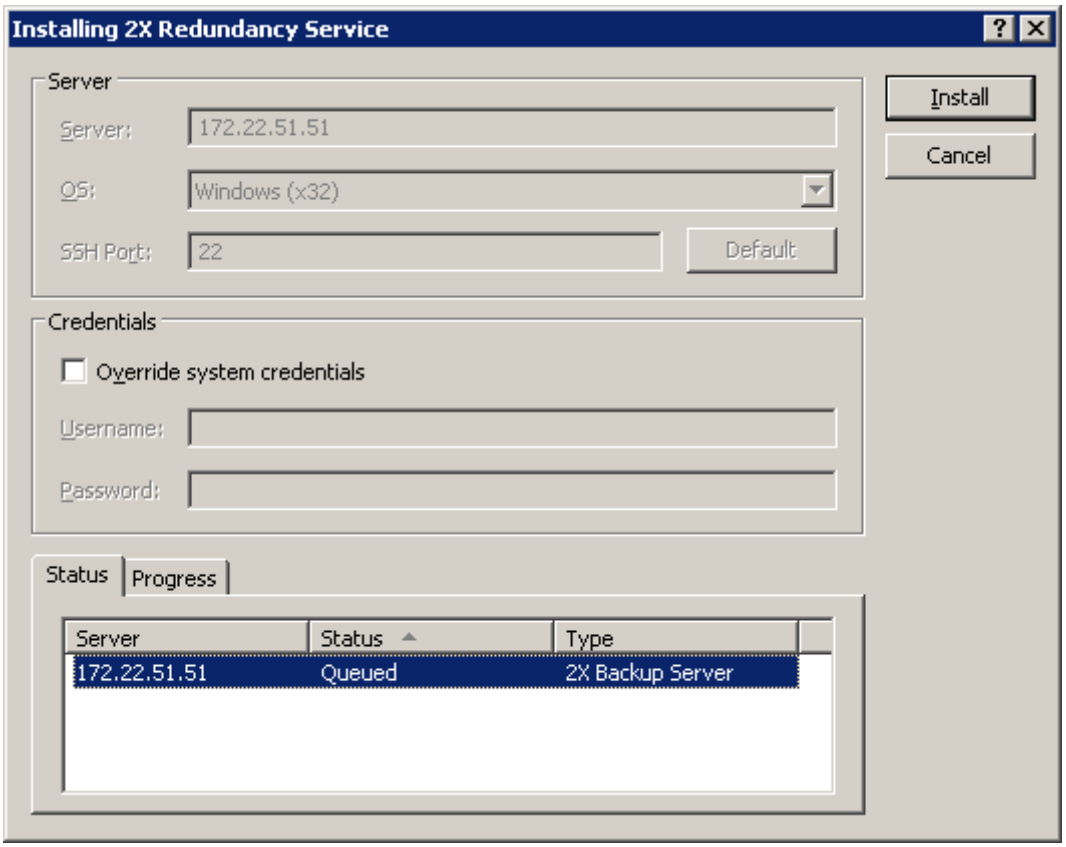
Configuring Backup Servers for a Site

2. Click **Add** from the **Tasks** drop down to launch the Backup Server wizard. Specify the IP address of the server that will be the new backup server.

3. In the second step of the wizard you are prompted to install the 2X Backup Server service on the target server unless already installed. Click **Install** to install the backup service.

Note: If the server is currently used for some other role the option to take over will be available instead of install. If you want to take over the server to use it as a backup server, click the **Take Over** button.

4. In the **Installing 2X Redundancy Service** dialog highlight the server name on which the 2X Agent is to be installed.
5. (Optional) Tick the option “Override system credentials” to specify and use different credentials to connect to the server and install the 2X Agent as seen in the below screenshot.



Installing the 2X redundancy Service

6. Click **Install** to install the agent and click **Done** once it has been successfully installed.
7. Click **OK** to add the server to the farm.

Managing Backup Servers

Enabling or Disabling Backup Servers

To enable or disable a backup server from a site highlight the server name from the **Backup Servers** node in the navigation tree and tick or untick the tick box next to the server name.

Changing Backup Servers Priority

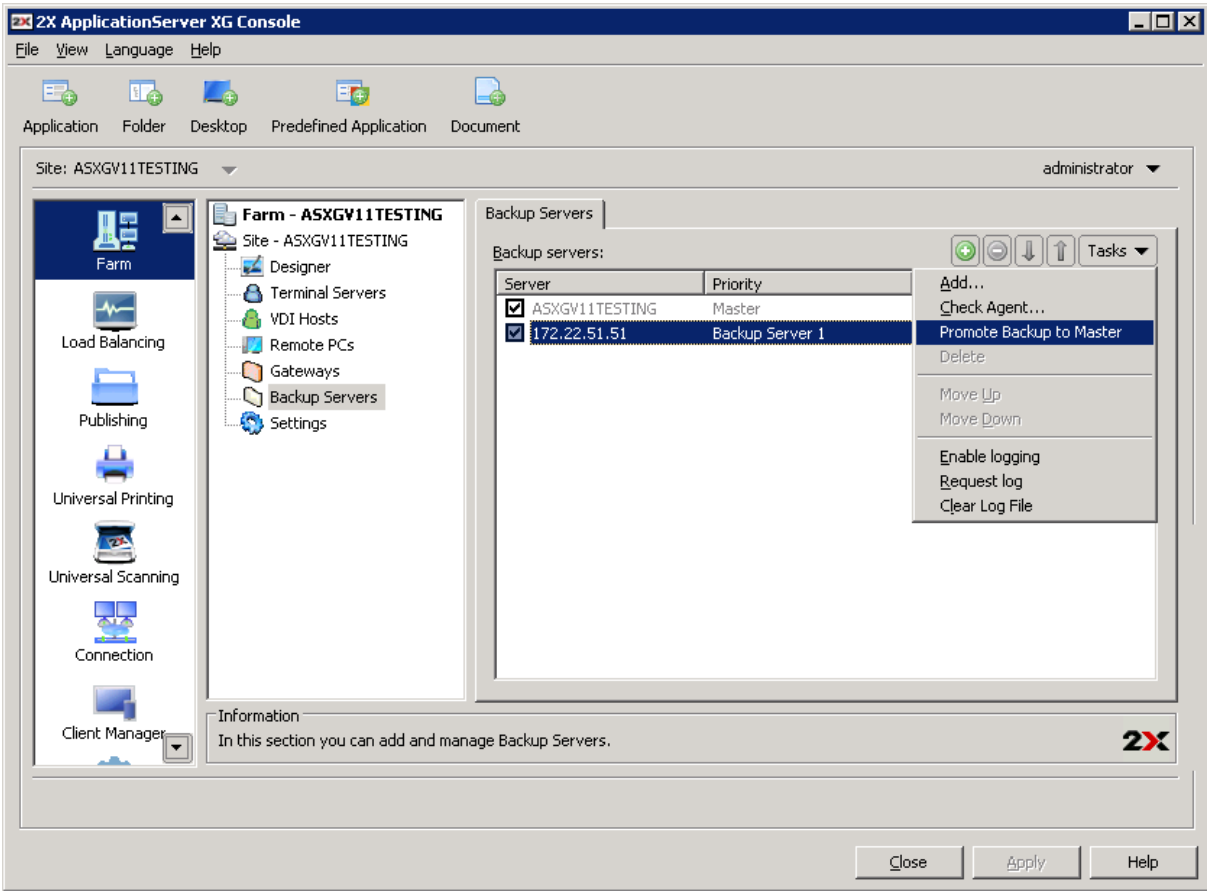
Each backup server in the list is given a priority. By default, the local 2X Publishing agent is given the Master priority which cannot be changed. To change the priority of other backup

servers in the farm, highlight the server name and use the **Move Up** and **Move Down** buttons to assign the correct priority.

Promoting a Backup Server to Master Server

In case the primary server cannot be recovered you can promote a 2X Backup Server to a Master Server by following the below procedure:

1. Open the 2X ApplicationServer Console on the server which you would like to promote. (all required files are automatically installed when a server is added as a backup server)
2. Open the **Farm** category and navigate to the **Backup Servers** node, highlight the server name and from the **Tasks** drop down menu click **Promote Backup to Master** as seen in the below screenshot.



Promoting a Backup Server to Master

3. Click **OK** once the process is finished.

Deleting Backup Servers

To delete a backup server highlight the server name and click the **Delete** button or press the **Delete** / **Del** key on the keyboard.

Load Balancing

Introduction

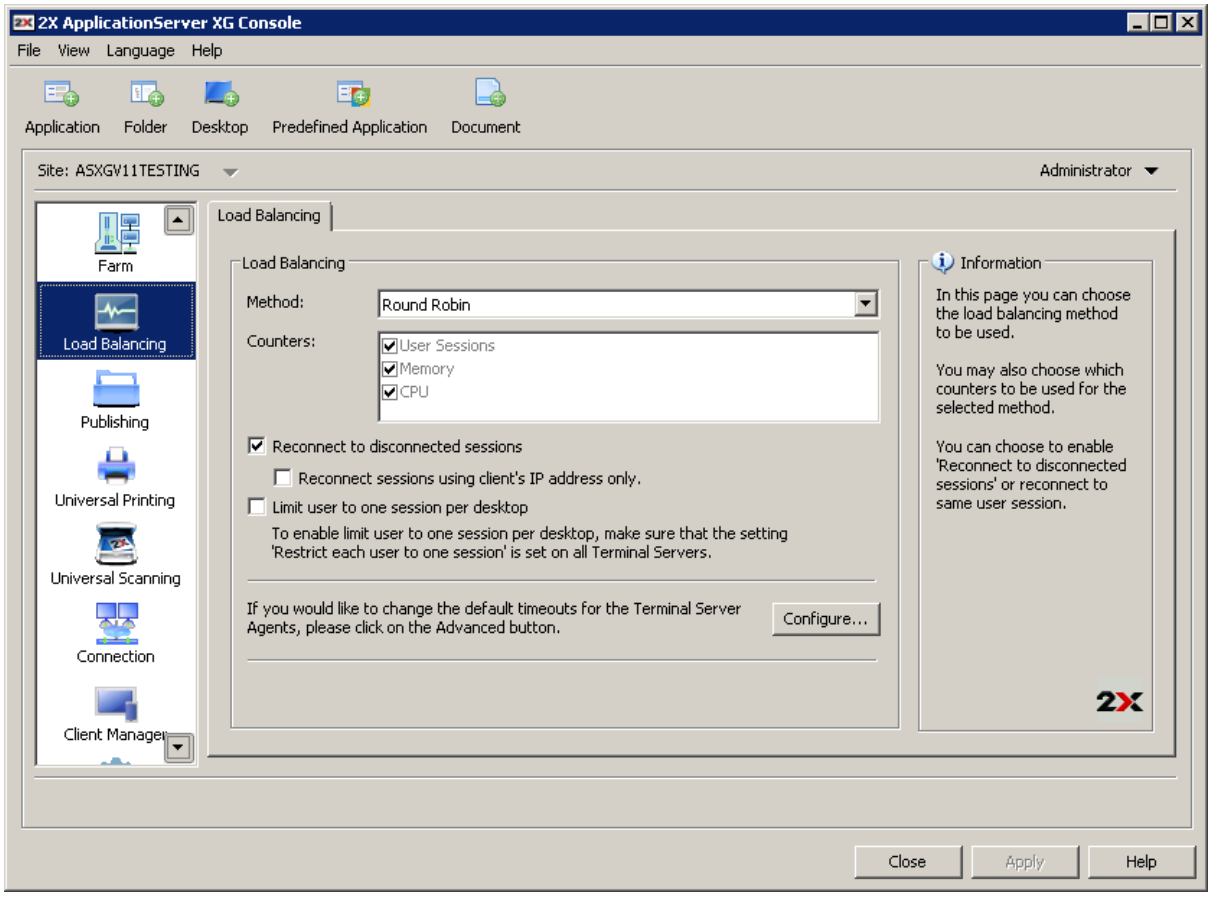
The 2X Load Balancer is designed to balance RDS and VDI Hosts connections made from 2X ApplicationServer XG Clients. There are 2 types of load balancing methods available:

- Resource Based
- Round Robin

Resouce Based load balancing distributes sessions to servers depending on how busy the servers are. Therefore a new incoming session is always redirected to the least busy server.

Round robin load balancing redirects sessions in sequential order. For example the first session is redirected to server 1, the second session is redirected to server 2 and the third session is redirected to server 1 again when there are two terminal servers in the farm.

Both methods are explained in this chapter. The load balancing options can be configured from the **Load Balancing** category in the navigation bar.


2X ApplicationServer XG Console
File View Language Help
Application
Folder
Desktop
Predefined Application
Document
Site: ASXGV11TESTING
Administrator
Farm
Load Balancing
Publishing
Universal Printing
Universal Scanning
Connection
Client Manager
Load Balancing
Load Balancing
Method:
Round Robin
Counters:
User Sessions
Memory
CPU
Reconnect to disconnected sessions
Reconnect sessions using client's IP address only.
Limit user to one session per desktop
To enable limit user to one session per desktop, make sure that the setting 'Restrict each user to one session' is set on all Terminal Servers.
If you would like to change the default timeouts for the Terminal Server Agents, please click on the Advanced button.
Configure...
Information
In this page you can choose the load balancing method to be used.
You may also choose which counters to be used for the selected method.
You can choose to enable 'Reconnect to disconnected sessions' or reconnect to same user session.
Close
Apply
Help

Load Balancing Category

Resource Based Load Balancing

Enabling Resource Based Load Balancing

Load balancing is enabled by default when more than one server is available in the site. The resource based load balancing is the default method.

To switch back to resource based from round robin load balancing, select **Resource Based** from the **Method** drop down menu.

Configuring Resource Counters

Resource based load balancing uses the below list of counters to determine if a server is busier than the other/s and vice versa:

- **User sessions:** redirect users to a server with the least number of sessions
- **Memory:** redirect users to the server with the best free/used RAM ratio
- **CPU:** redirect users to the server with the best free/used CPU time ratio

When all the counters are enabled, the 2X LoadBalancer adds the counter ratios together and redirects the session to the server with the most favourable combined ratio.

To remove a counter from the equation, untick the check box next to the counter name in the **Counters** section. To add it back to the equation, tick back the check box.

Round Robin Load Balancing

Round robin load balancing redirects sessions in sequential order. For example with 2 RDS servers in the farm, the first session is redirected to server 1, the second session is redirected to server 2 and the third session is redirected to server 1 again.

Enabling Round Robin Load Balancing

To enable round robin load balancing select **Round Robin** from the **Method** drop down menu in the Load Balancing section.

Advanced Load Balancing Settings

Session Management

Reconnect Disconnected Sessions

Enable the option **Reconnected to disconnected sessions** in the **Load Balancing** tab to redirect incoming user sessions to a previously disconnected session owned by the same user.

Reconnect sessions using client's IP address only

When reconnecting to a disconnected session the 2X ApplicationServer XG will match the username requesting to reconnect with the username of the disconnected session to match the sessions. With this option enabled, the 2X ApplicationServer will determine to which disconnected session to reconnect the session by matching the source IP.

Limit Number of Sessions for Users

Enable this option to ensure that the same user does not open multiple sessions.

Configure Servers Connection and Uptime Test

To prevent connections being sent to an RDS server which is not responding, the 2X ApplicationServer XG frequently checks that the terminal server agent is still responding. You can configure the time intervals of such tests by clicking the **Configure** button at the bottom of the **Load Balancing** tab. The options are:

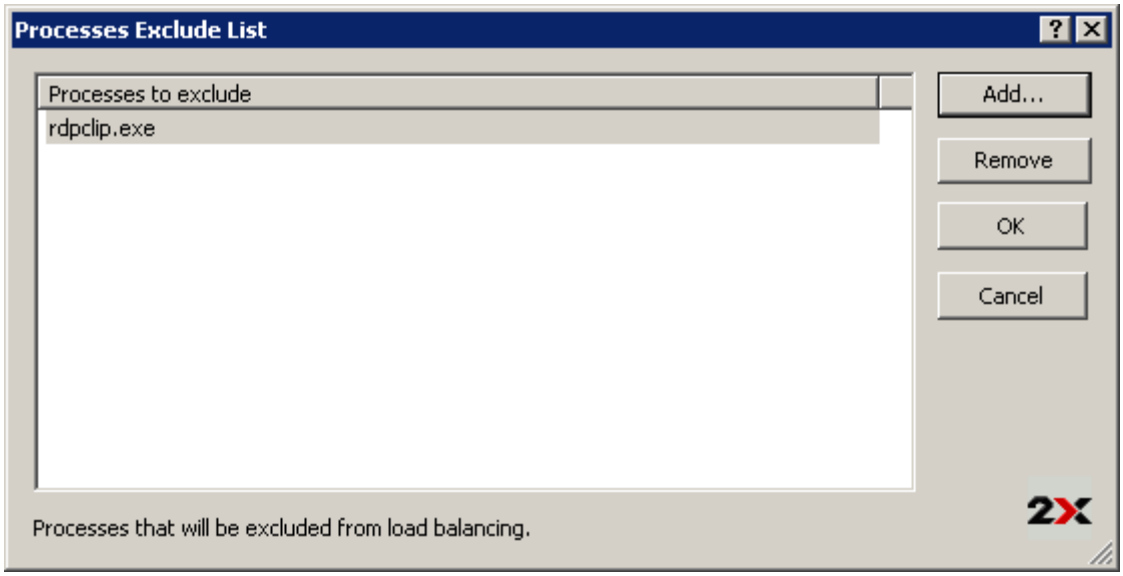
Declare TS Agent dead if not responding: specify the number of seconds needed for a non responding server to be declared as dead and have it excluded from the load balancer.

TS Agent Refresh Time: specify the number of seconds needed for the 2X ApplicationServer XG to check if the terminal server agent is reachable.

Excluding a Process from the CPU Counter

To exclude a process so it does not affect the free/used CPU time ratio on a server follow the procedure below:

- Click the **Configure** button at the bottom of the Load Balancing options.
- Tick the option **Enable CPU Load Balancer** and click **Exclude List.**



Excluding a Process from Load Balancing

- Click **Add** to select a process from the list of running processes. Alternatively you can specify a process name in the **Please Enter Process Name** input filed at the bottom of the dialogue box.
- Click **OK** to close the **Processes Exclude List** dialogue box or **Add** to add other processes.

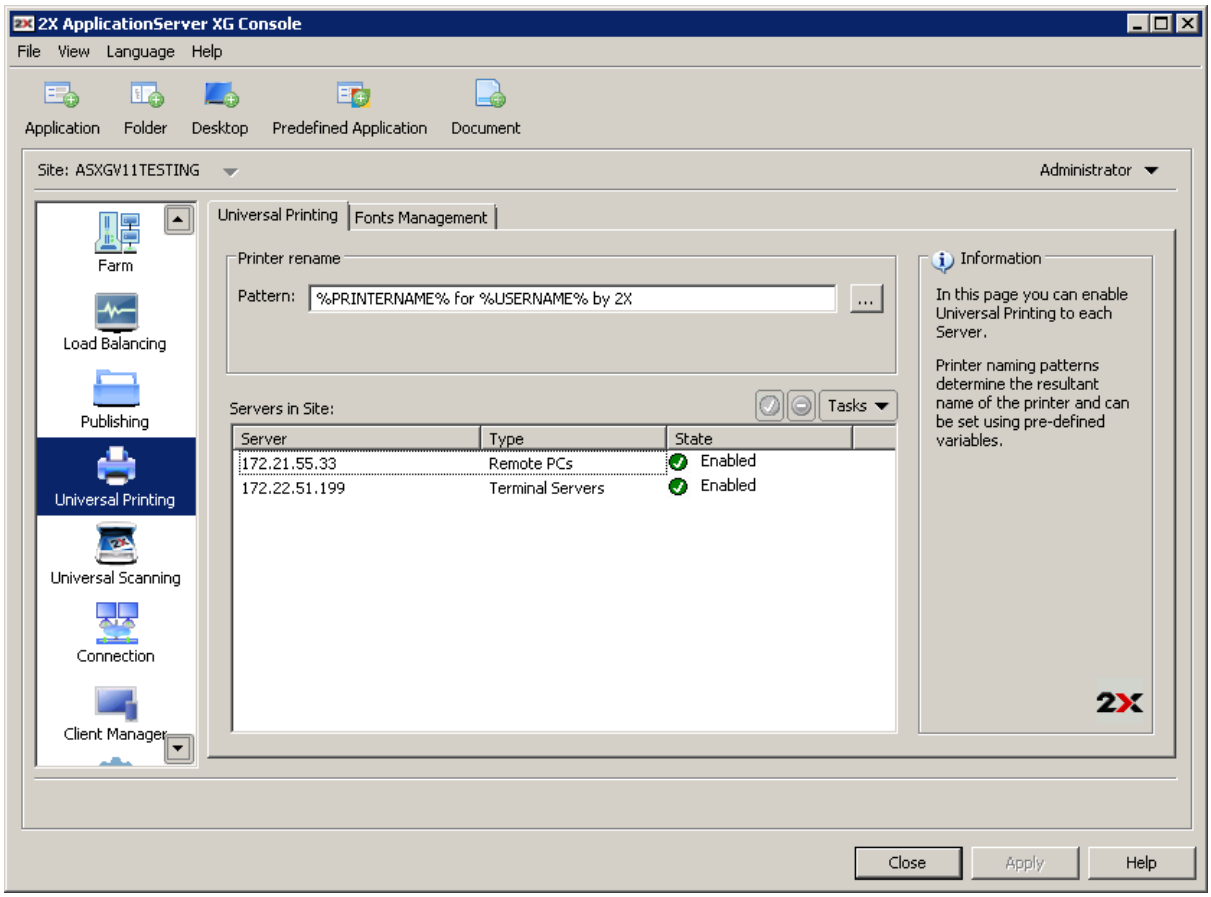
To remove a process from the processes excluded list highlight the process and click **Remove**.

2X Universal Printing

Introduction

Printer redirection enables users who are connected to a remote desktop or accessing a published application to print on their locally installed printer.

2X Universal Printing simplifies the printing process and solves most printer driver problems by not requiring that the server has a printer driver for the user's locally installed printer. Therefore a user can always print irrelevant of the type and brand of printer installed on the machine and the administrator does not have to install a printer driver for each different printer on the network.



Configuring Universal Printing

Managing 2X Universal Printing Servers

By default the 2X Universal Printing driver is automatically installed with the Terminal Server, VDI Guest and Remote PC agents. Therefore upon adding a server to the farm the 2X

Universal Printing is installed. The 2X Universal Printing driver is available in 32 and 64 bit format.

Enabling and Disabling the 2X Universal Printing Support

To enable or disable the 2X Universal Printing support for a particular server follow the below procedure:

1. Open the 2X ApplicationServer Console and select the **Universal Printing** category.
2. Highlight the name of the server you would like to modify from the **Servers in Site** list and click **Enable** to enable the 2X Universal Printing support or **Disable** to disable it from the **Tasks** drop down menu.

Configuring a Printer Renaming Pattern

By default 2X ApplicationServer renames the printers using the following pattern: **%PRINTERNAME% for %USERNAME% by 2X**. Therefore if a user Robert that has PRINTER1 installed locally connects to a remote desktop or published application, his printer is renamed to **PRINTER1 for Robert by 2X**.

To change the pattern used to rename printers specify a new pattern in the **Printer rename pattern** input field found in the 2X ApplicationServer Console > **Universal Printing** node. The variables available for renaming printers are:

- **%PRINTERNAME%**: client side printer name
- **%USERNAME%**: username of the user connected to the server
- **%SESSIONID%**: session ID of the action session
- **<2X Universal Printer>**: Legacy mode. This means that only one printer name will appear and be used, even when a user has multiple printers installed locally. In this mode the virtual printer does not have the same hardware characteristics of the local printer.

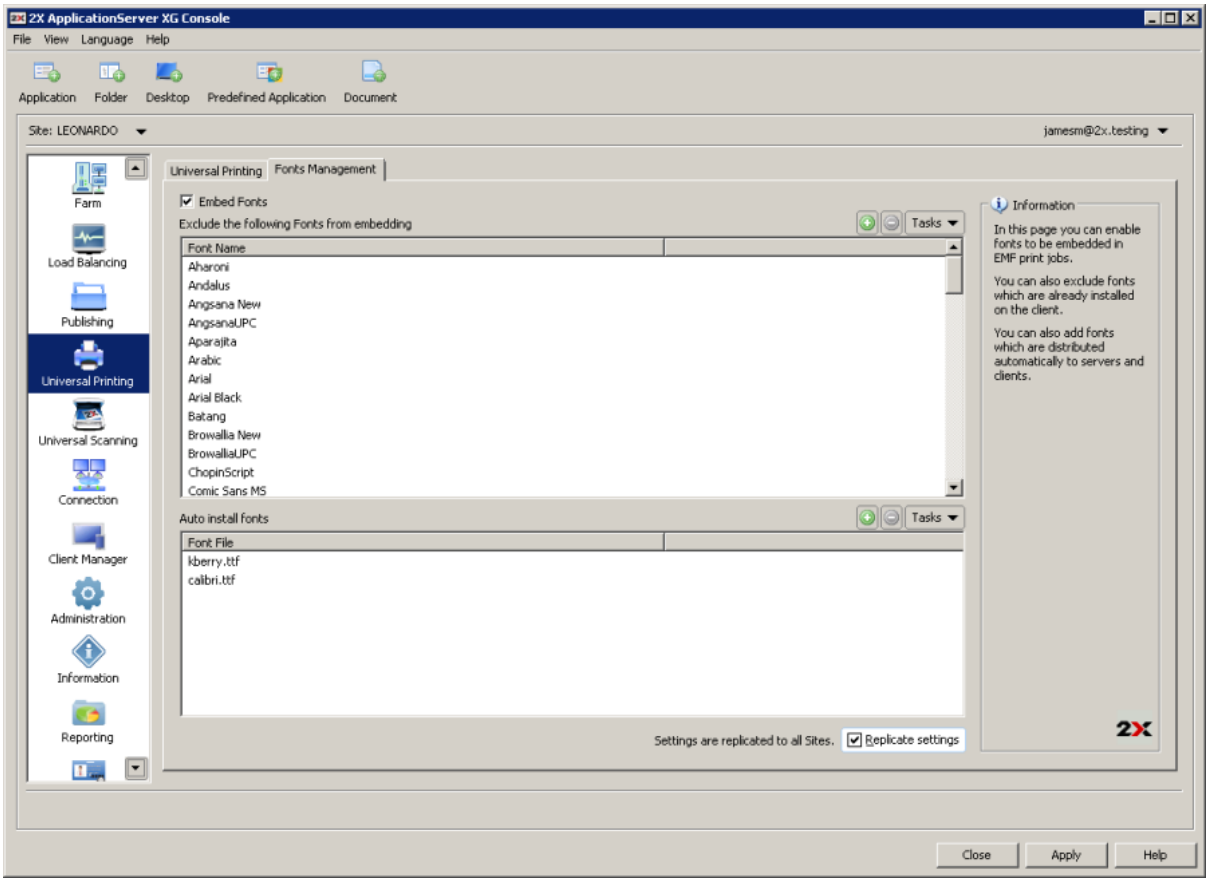
You can also configure a different printer renaming pattern specifically for each server from the server properties.

Note: Redirected printers are only accessible by administrator and the user who redirected the printer.

Fonts Management

Fonts need to be embedded so when printing a document using 2X Universal Printing, the document is copied to the local spooler of the client machine to be printed. If the fonts are not present on the client machine the print out would not be correct.

To control the embedding of fonts within a print job use the **Fonts Management** tab and check/uncheck the option **Embed Fonts**.



Embed Fonts Options

Excluding Fonts from Embedding

To exclude a specific font type from being embedded, click **Add** from the **Tasks** drop down menu in the **Exclude the following Fonts from embedding** section and select a font from the list.

Automatically Install Fonts on Servers and Clients

To automatically install a specific font type on servers and clients click **Add** from the **Tasks** drop down menu in the **Auto install fonts** section and select the fonts from the list.

Note: By default fonts added to the auto install list will be excluded from the embedding list because the fonts would be installed on the Windows clients, therefore there is no need for them to be embedded. Untick the option **Automatically exclude font from embedding** in the **select font** dialog box so the font is not excluded from the embedding list.

Resetting List of Excluded Fonts to Default

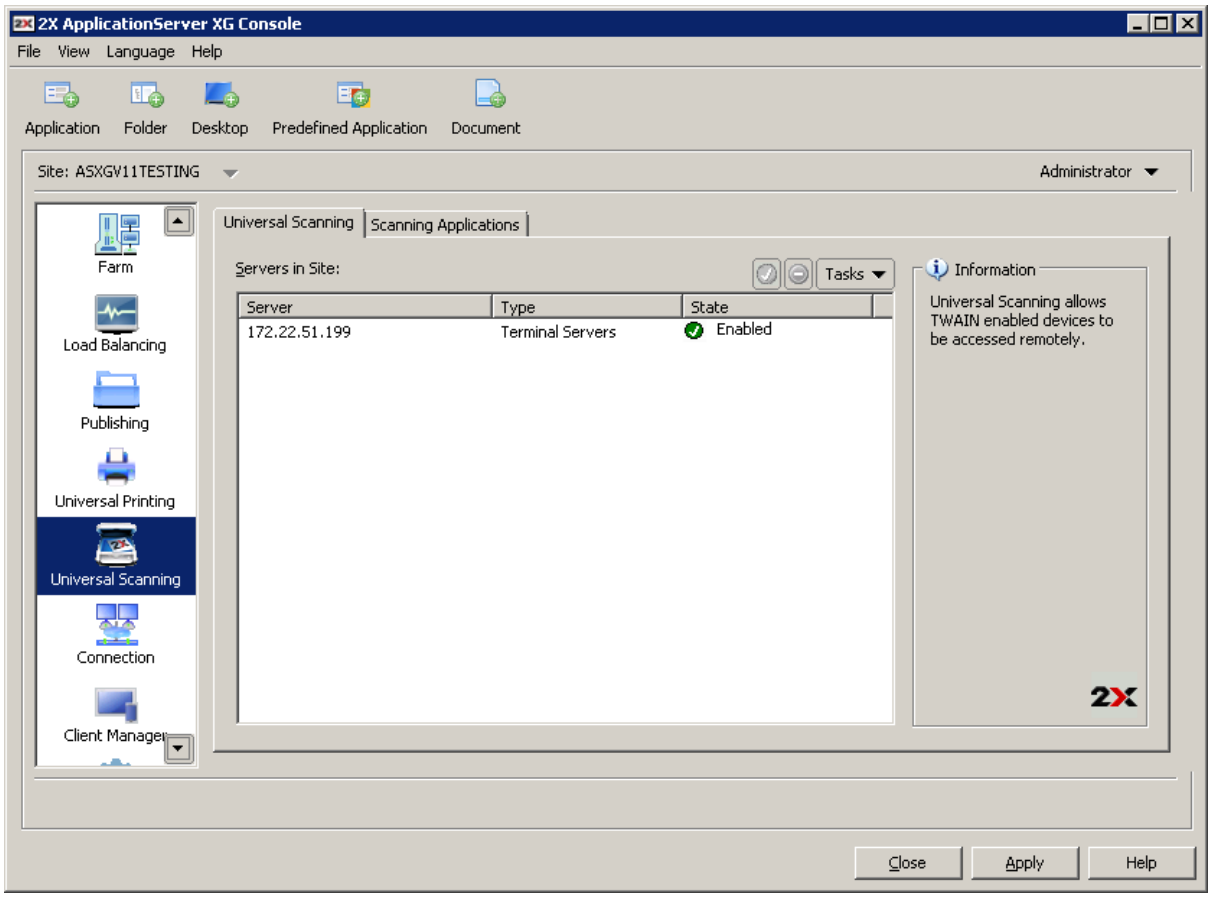
To reset the list of excluded fonts to default click **Reset to Default** from the **Tasks** drop down menu.

2X Universal Scanning

Introduction

Scanner redirection enables users who are connected to a remote desktop or accessing a published application to make a scan using the scanner that is connected to the client machine.

2X Universal scanning uses TWAIN redirection to let any application using TWAIN technology use hardware connected to the client device for scanning. With 2X Universal Scanning there is no need to install any scanner driver on the server. Only one scanner is shown on the server regardless of the number of users and sessions currently in use on the terminal server.



Universal Scanning Options

Managing 2X Universal Scanning

By default the 2X Universal Scanning driver is automatically installed with the Terminal Server, VDI Guest and Remote PC agents. Therefore upon adding a server to the farm the 2X Universal Scanning is installed.

Note: The 2X Universal Scanning driver is available in 32 and 64 bit format. Currently only 32 bit applications are supported.

Enabling and Disabling 2X Universal Scanning Support

To enable or disable the 2X Universal Scanning support from a particular server follow the below procedure:

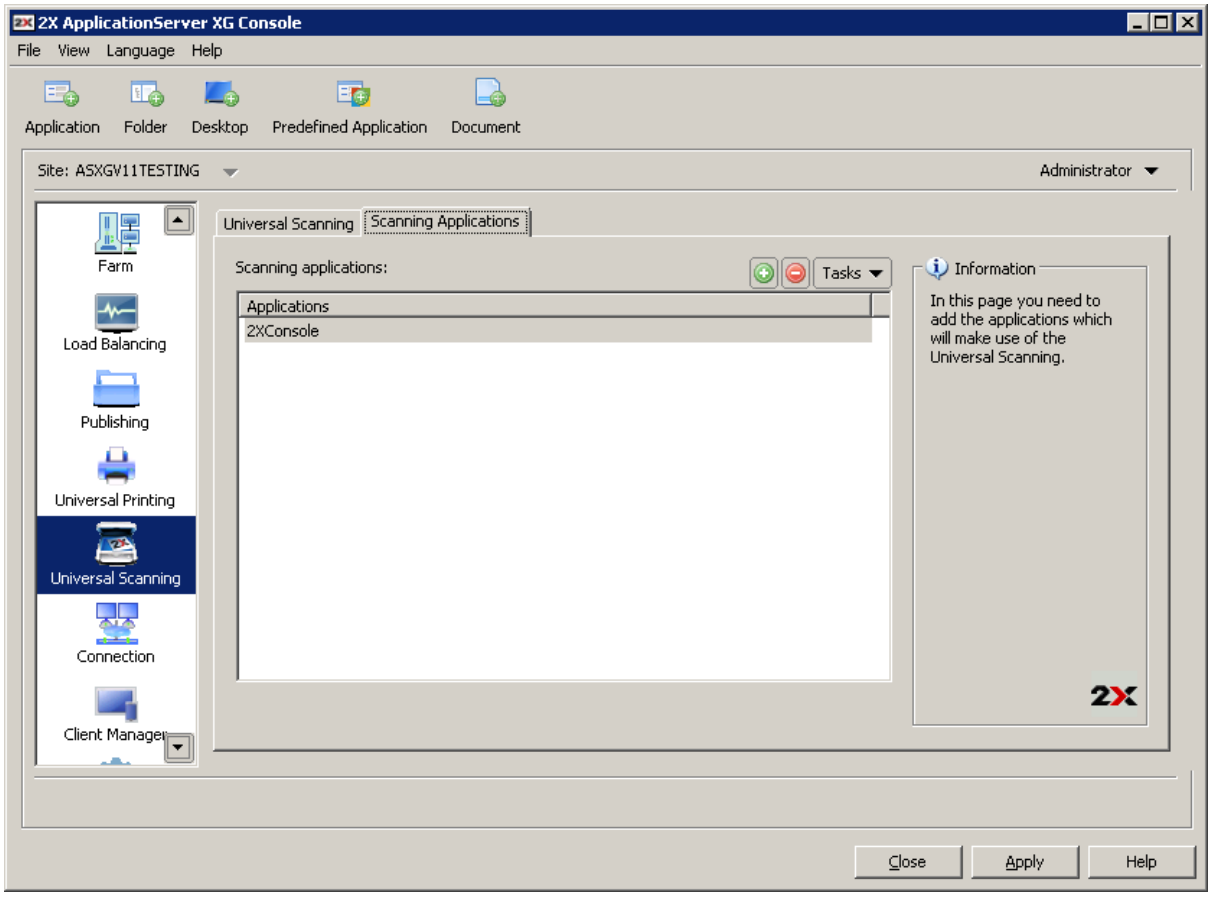
1. Open the 2X ApplicationServer console and open the **Universal Scanning** category in the navigation bar.
2. Highlight the name of the server you would like to modify and click **Enable** to enable 2X Universal Scanning support or **Disable** to disable it from the **Tasks** drop down menu.

Managing Scanning Applications

Adding a Scanning Application

Applications that will use the Universal Scanning feature have to be added in the **Scanning Applications** tab so they can use the Twain driver, hence making it easier for the administrator to set them up. Follow the below procedure to add an application to the list of Scanning applications:

1. Open the 2X ApplicationServer console and open the **Universal Scanning** category.
2. Click on the **Scanning Applications** tab and click **Add**.
3. Browse to the application executable and click **Open**.



Configuring Scanning Applications

Note: Some applications might use different or multiple executables. Make sure that all used executables are added to the list of scanning applications.

Deleting a Scanning Application

To delete a scanning application from the list highlight the application name and click **Delete** from the **Tasks** drop down menu.

Note: By deleting an application from the list of scanning applications the installation of the application will not be affected.

Installing 2XOS and Network Booting

Introduction

The 2XOS is a proprietary Debian based operating system which can be installed in a standalone mode on Thin Clients or used for network booting. It offers standalone RDP and the ability to connect to a 2X ApplicationServer XG.

Network Booting a Device Running 2XOS

To be able to network boot devices running the 2XOS on the 2X ApplicationServer XG farm follow the below procedure.

1. Configure Thin Client Support on Gateway

Enable Thin Client support on the gateway as explained in section **Configuring Thin Client and 2XOS Support** on page 100.

Note: Unless you will manually configure the DHCP ensure that the option DHCP Proxy is enabled.

2. Choose and Install the Required 2X Operating System(s)

There are 9 flavours of the operating system which can be divided into 3 categories; Generic, Compact and Hypervisor version.

The Generic is the full operating system while the Compact has limited features and should be used on devices with low specifications. The Hypervisor versions are to be used on the specific hypervisors namely VMWare, HyperV and VirtualBox.

The generic and compact versions come in 3 revisions; R3 should be used over Intel, ATI, Nvidia, SiS and SiS Mirage chipsets. R2 should be used with VIA Chrome9 chipsets. R1 is used for older chipsets such as VIA Unichrome and Geode.

Use the operating sytem that matches the device Chipset. If you do not know which one is available on your device or you selected the wrong one, the OS will report you the correct Revision to use once booted.

Choose and Add the 2XOS

To choose and add a version of 2XOS to the 2X ApplicationServer XG follow the procedure **Making a Version of 2XOS Available for Thin Clients** on page 128. The first added operating system will be the default OS unless changed.

Configure the Thin Client Group

Also check that the <default> thin client group is configured with **Allow** permissions and the hardware boot method is set to **Network Boot**. For more information on thin client groups refer to the section **Thin Clients Groups** on page 131.

3. Configure the Device and Boot It

Boot the PC or Thin Client and configure the BIOS setting s so that it does a Network boot. These settings might vary from one device to another. Continue booting up the device and the device information will appear in the Devices page with the current state of the device.

Note: If you plan to network boot multiple devices it is recommended not to boot more than 50 devices together but to configure unattended automatic boot events via the scheduler.

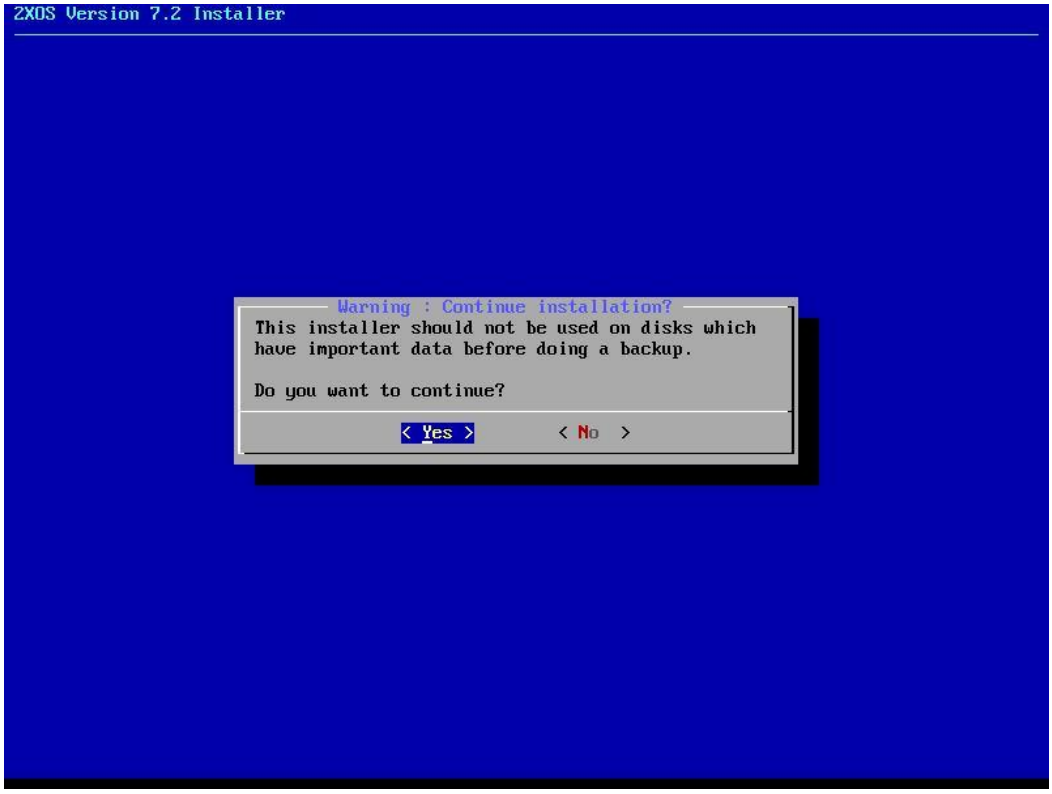
Installing 2XOS on Thin Client or PC Permanent Storage

There are 2 different ways how to install the 2XOS on a permanent storage:

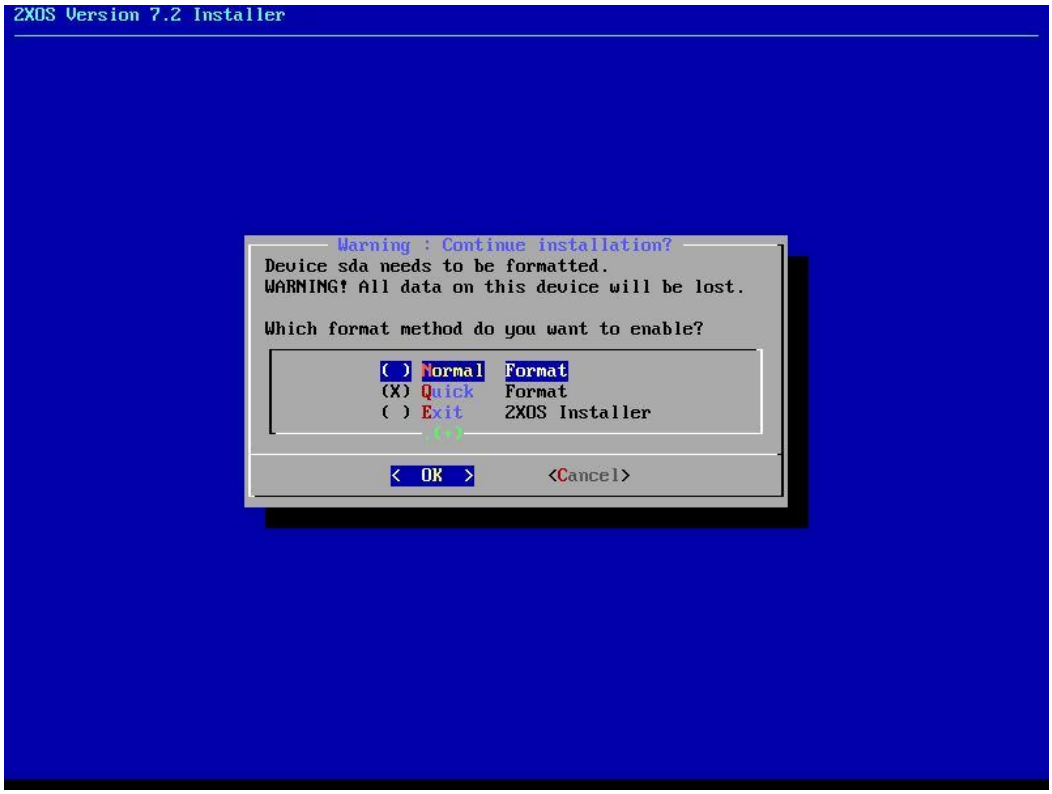
1. Burn a CD with the 2XOS ISO downloaded from the 2X website. Boot the device from the CD and follow the installer instructions after choosing the (installer) option. Choose the storage where the 2XOS is to be installed and proceed with the installation.
2. Follow the procedure **Network Booting a Device Running 2XOS** and in step 3 select the option **Install (Attended)**. Proceed by following the installer instructions and choosing the storage where the 2XOS is to be installed.

GNU GRUB version 2.00
Vmware-v7.2_release-r11489 (Live CD)
Vmware-v7.2_release-r11489 (Live CD) - Safe Mode
Vmware-v7.2_release-r11489 (Hardware Profile)
Vmware-v7.2_release-r11489 (Hardware Profile) - Safe Mode
Vmware-v7.2_release-r11489 (Installer)
Vmware-v7.2_release-r11489 (Installer) - Safe Mode
Boot From Local Drive
Network Boot
Memory Burn-In Test
2XOS
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c'
for a command-line.

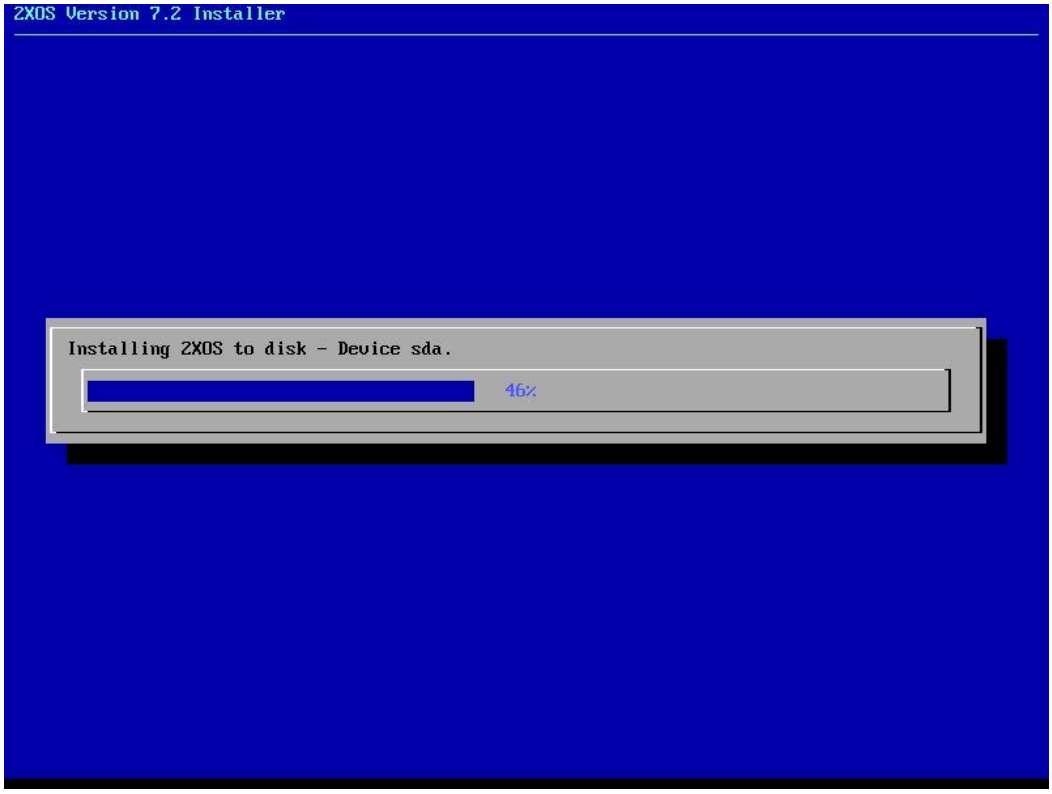
2XOS Installation Menu


2XOS Version 7.2 Installer
Warning : Continue installation?
This installer should not be used on disks which
have important data before doing a backup.
Do you want to continue?
< Yes >
< No >

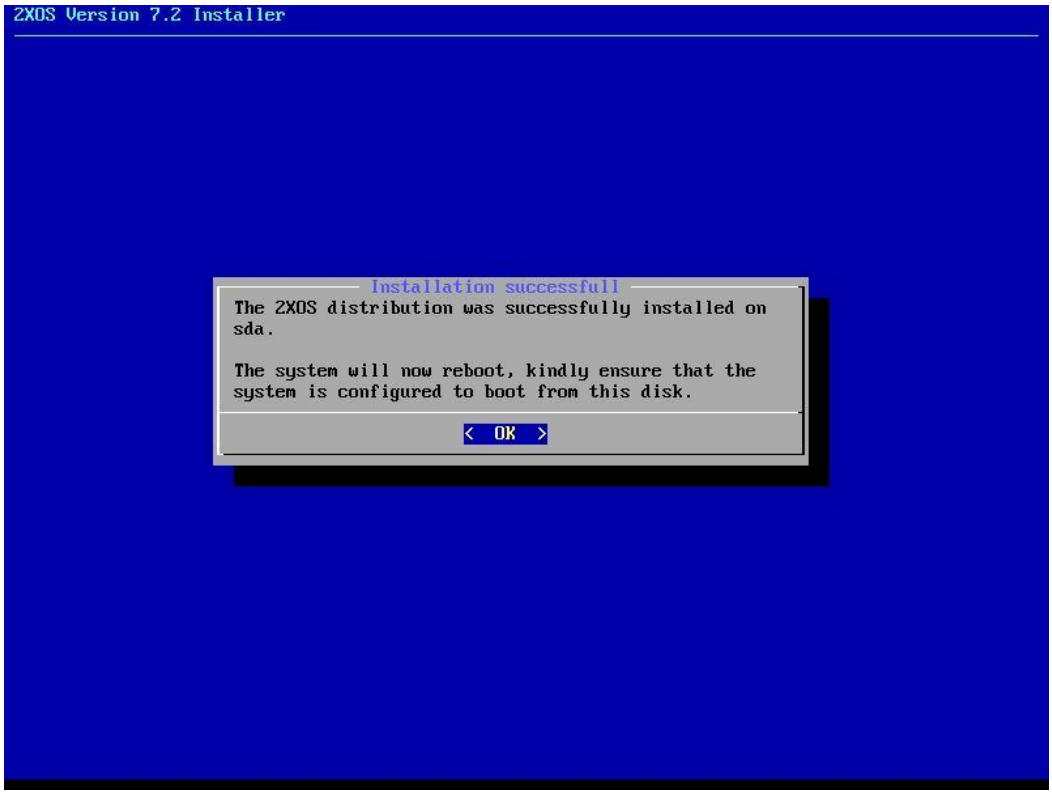
Installing 2XOS on a Permanent Storage will Erase all Data on the Storage


2XOS Version 7.2 Installer
Warning : Continue installation?
Device sda needs to be formatted.
WARNING! All data on this device will be lost.
Which format method do you want to enable?
( ) Normal Format
(X) Quick Format
( ) Exit 2XOS Installer
< OK >
<Cancel>

Specifying Format Method to be used during 2XOS Installation



Installing 2XOS to Permanent Storage


2XOS Version 7.2 Installer
Installation successfull
The 2XOS distribution was successfully installed on sda.
The system will now reboot, kindly ensure that the system is configured to boot from this disk.
< OK >

Installation of 2XOS Successfully Finished

Unattended Install of 2XOS on Thin Client or PC Permanent Storage

If you need to install 2XOS on the permanent storage of multiple devices, 2X ApplicationServer XG version 11 and 2X OS 7.3 have a new Boot Method called **Install (Unattended)**. When selected, it will automatically install the 2XOS on the first permanent storage where the 2XOS can fit.

Note: When this option is used, any data on the drive is overwritten without any warning.

Creating a Bootable USB Stick That Matches Your Device

There are 2 different ways how to install the 2XOS on a permanent storage:

1. Burn a CD with the 2XOS ISO downloaded from the 2X website. Boot the device from the CD and follow the installer instructions after choosing the (installer) option. Choose the USB device where the 2XOS is to be installed and proceed with the installation.
2. Follow the procedure **Network Booting a Device Running 2XOS** and in step 3 select the option **Install (Attended)**. Proceed by following the installer instructions and choosing the storage where the 2XOS is to be installed.

Managing Devices and Thin Clients

Introduction

From the **Client Manager** category in the 2X ApplicationServer Console you can view all clients connected to the system, manage and deploy 2X ApplicationServer components to Thin Clients running the 2XOS. You can also limit and enforce the configuration of the Windows 2X Client.

Note: The Client Manager module is able to manage clients running 2XOS machine running v7.2 or later.

Monitoring Devices

Introduction

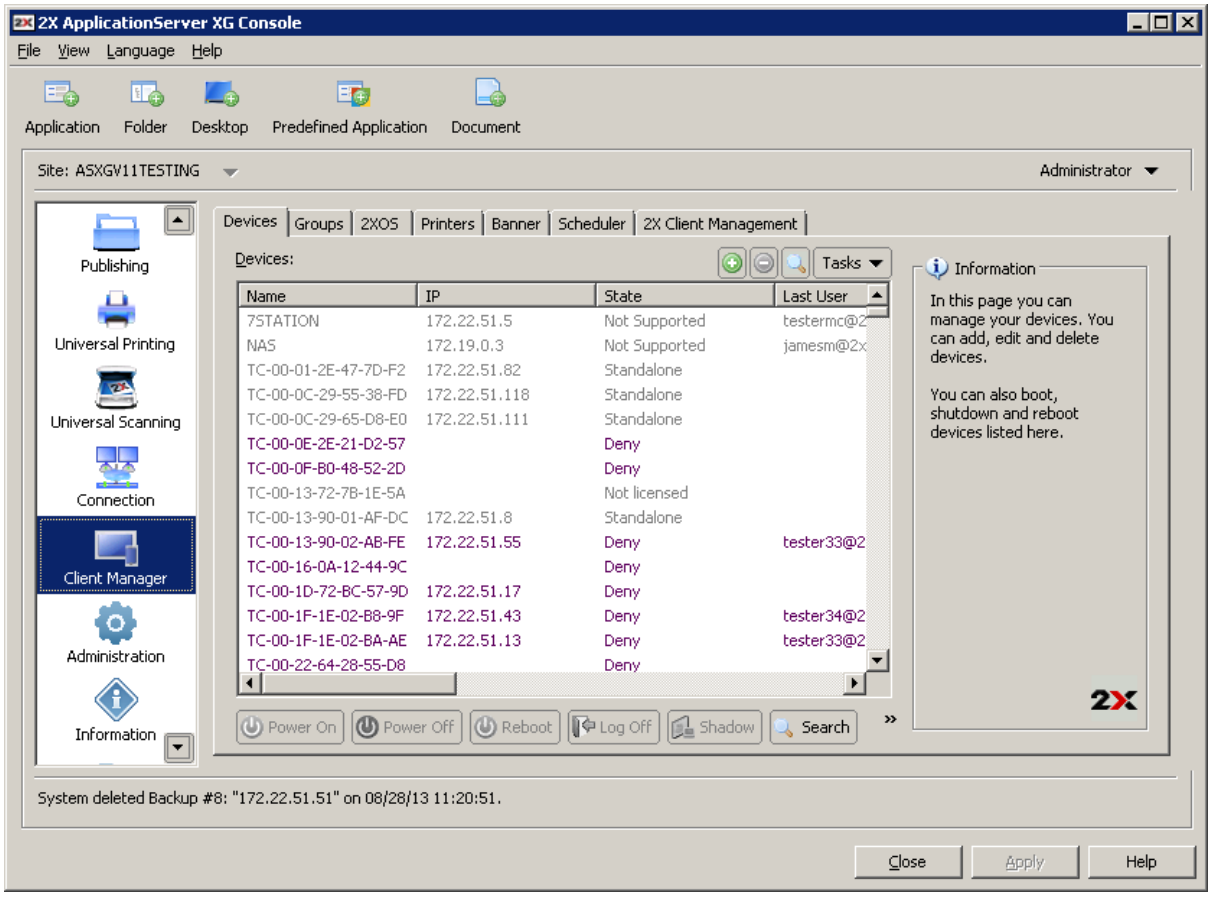
From the **Devices** tab in the **Client Manager** category you can get an overview of all the clients that connect to the 2X ApplicationServer XG. From the same tab you can also search for devices that connect to the 2X ApplicationServer XG and also power on or off, reboot, logoff devices running the 2XOS using the **Device Toolbar** at the bottom. The following information is available for each device:

- Name
- IP Address
- State of device (more information about device status in the following section)
- Last user that used the device
- OS Version

Device Statuses

Devices and thin clients that connect to the 2X ApplicationServer XG can have any of the following states:

- **Off**: Device is switched off
- **Booting**: Device is booting
- **Installing**: Device is installing
- **Connected**: Device is connected
- **Logged On**: Devices is logged on to the system
- **Restarting**: Device is restarted
- **Standalone**: Device has previously connected to the 2X ApplicationServer XG but is not using 2XOS, therefore it cannot be managed
- **Needs Approval**: Device needs approval to connect to the 2X ApplicationServer
- **Deny**: Device has been denied access to the 2X ApplicationServer
- **Not Support**: Device is not supported by the 2X ApplicationServer
- **Not Licensed**: Device is not licensed
- **Error**: Device is experiencing errors



Devices Listed in the Client Manager Category

2XOS

Introduction

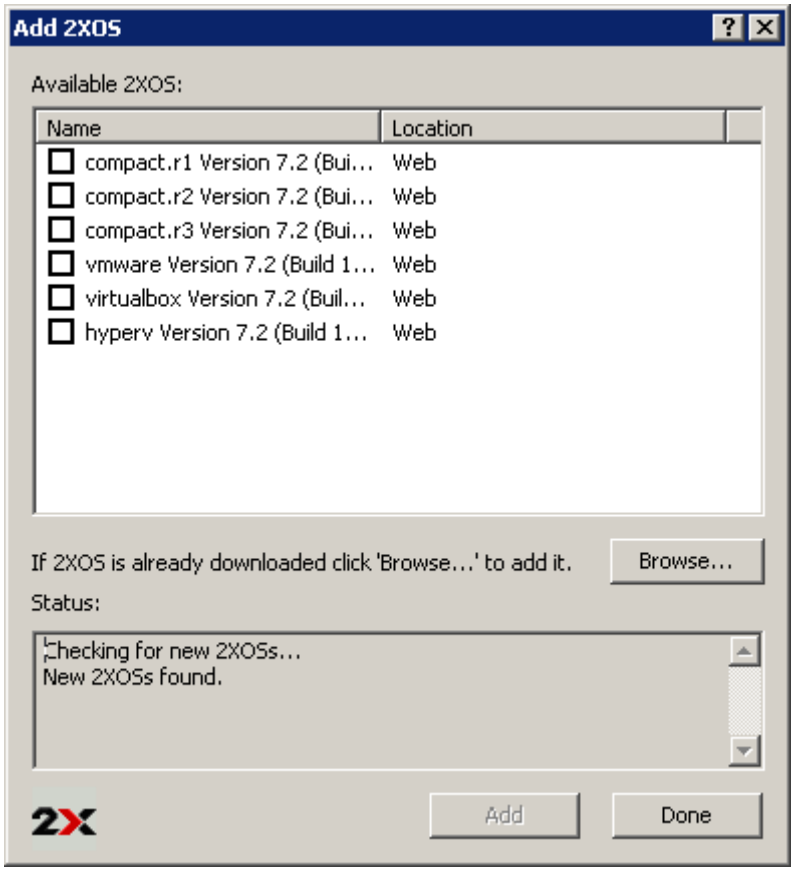
The 2XOS is a proprietary Debian based operating system which can be installed in a standalone mode on Thin Clients, offering standalone RDP and the ability to connect to a 2X ApplicationServer XG. Before adding any hardware (Thin Clients) to the **Client Manager** to manage and assign a 2XOS to, you should configure the 2XOS builds which the Thin Clients will download.

Making a Version of 2XOS Available for Thin Clients

To add a 2XOS to the 2X ApplicationServer and make it available for Thin Clients navigate to the **2XOS** tab in the **Client Manager** category and click **Add** from the **Tasks** drop down menu.

- Tick the checkbox next to the 2XOS version you would like to download and click the **Add** button. Once downloaded click **Done** so it is added to the list of available operating systems for clients.

- If you have already downloaded a copy of the 2XOS, click th **Browse** button to the 2XOS zip file and click **Open** to add it to the list of available operating systems. Click **Done** when ready.



Adding a 2XOS to the List of Available Operating Systems for Clients

Note: You can download a version of the 2XOS from the 2XOS download page: http://www.2x.com/os/downloadlinks/.

Once the 2XOS is added to the **List of thin client operating systems**, it can be downloaded and used by thin clients on the network. To configure the 2X ApplicationServer XG to support thin clients refer to the section Configuring Thin Client and 2XOS Support on page 100.

Configuring a Version of the 2XOS as Default

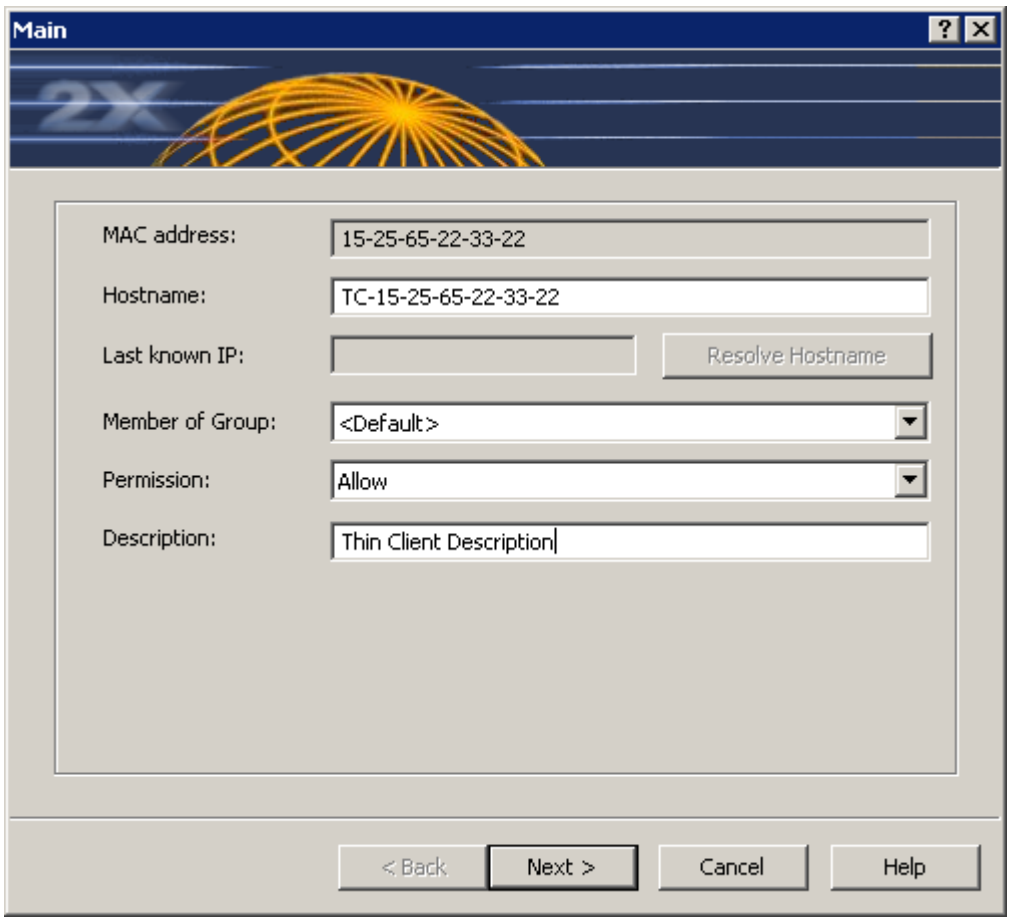
Navigate to the **2XOS** tab in the **Client Manager** category and highlight the 2XOS name and click **Set Default** from the **Tasks** drop down menu. Therefore if a 2XOS has not been configured for a specific thin client, the default 2XOS will be used.

Adding a Thin Client

To manually add a device to run the 2XOS follow the below procedure:

3. Navigate to the **Devices** tab in the **Client Manager** category and click **Add** from the **Tasks** drop down menu**.**
4. In the first step of the wizard specify the MAC address of the device.
5. In the second step of the wizards specify the following:
    a. **Hostname**: If a hostname is not specified, a predefined name is automatically populated. Click the **Resolve Hostname** button to use the hostname of the last known IP of the device.
    b. **Group**: Use the **<default>** group if the device is not a part of any particular group. For more information about thin clients groups, refer to the section Thin Clients Groups on page 131.

c. **Permission**: Select **Allow** to allow the device to download the 2XOS. Select **Deny** to disallow the device from downloading and booting the 2XOS.
d. **Description**: Specify a friendly description.



Configuring a Thin Client's Group Membership and Permissions

6. From the third step onward or the wizard you can choose to manually configure any of the below options specifically for the device or configure the device to retrieve such settings from the group it was joined to.
    a. Hardware
    b. Auto login
    c. Regional settings
    d. Input devices
    e. Screen saver
    f. Desktop settings
    g. Browser settings
    h. Remote Desktop Client settings
    i. Kiosk Mode
    j. List of locally installed applications
    k. Shadowing options
    l. RDP default settings

Note: For more information about any of the above mentioned settings refer to the section Configuring Thin Client Options in Groups

on page 132.

7. Once ready click **Finish**.

Thin Clients Groups

Introduction

Thin Client Groups allow you to group a number of thin clients and manage them together. Therefore when a thin client boots and becomes part of a farm, the2X ApplicationServer XG will try to allocate the Thin Client into a group and the settings configured in such group are inherited by the thin client.

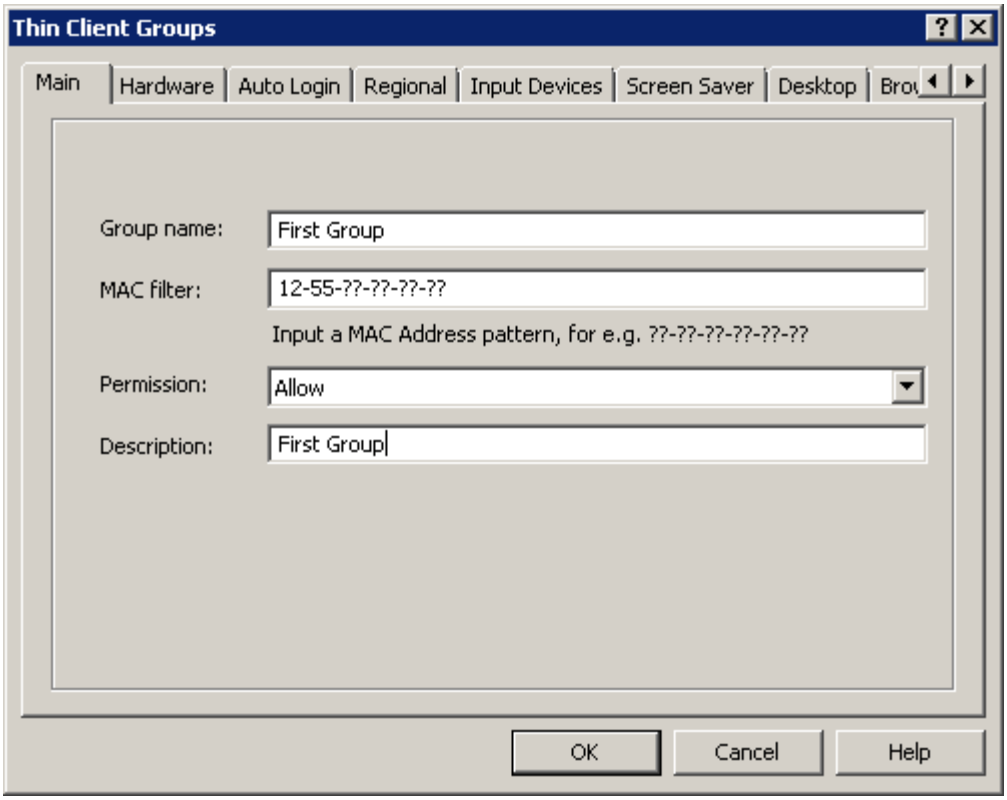
Note: Specific devices within a group might / can be configured to override inherited settings from the group.

If the thin client MAC address does not match any of the groups' MAC filters, the thin client is added to the default **<Default>** group that is configured to capture all devices automatically.

Creating a Thin Clients Group

To create a thin client group follow the below procedure:

1. Navigate to the **Groups** tab in the **Client Manager** category and click **Add** from the **Tasks** drop down menu.
2. In the **Main** tab specify the following:
    a. **Group Name**
    b. **MAC Filter**: The default filter (??-??-??-??-??-??) will match all devices. Different hardware has a consistent MAC address based on the hardware within it. Specify a wildcard based on the MAC addresses used by particular models to automatically enrol a specific range of thin clients to the group.
    c. **Permission**: Select **Allow** from the drop down menu so all thin clients in the group are allowed to boot and connect to the 2X ApplicationServer XG. Select **Deny** to deny the group of thin clients from downloading the 2XOS and connecting to the 2X ApplicationServer XG. If **Needs Approval** is selected any thin client which is enrolled to this group requires the administrator to manually allow or deny it. **Description**: Specify a user friendly description name for the group.



Configuring a Thin Client Group Name, MAC Filter and Permissions

Configuring Thin Client Options in Groups

In the thin client group you can also configure several options such as boot method, regional settings, input devices and more. All these settings will be automatically inherited to all the thin clients in the group. All of these options are listed in this section and can be accessed when creating a new group or from the group properties.

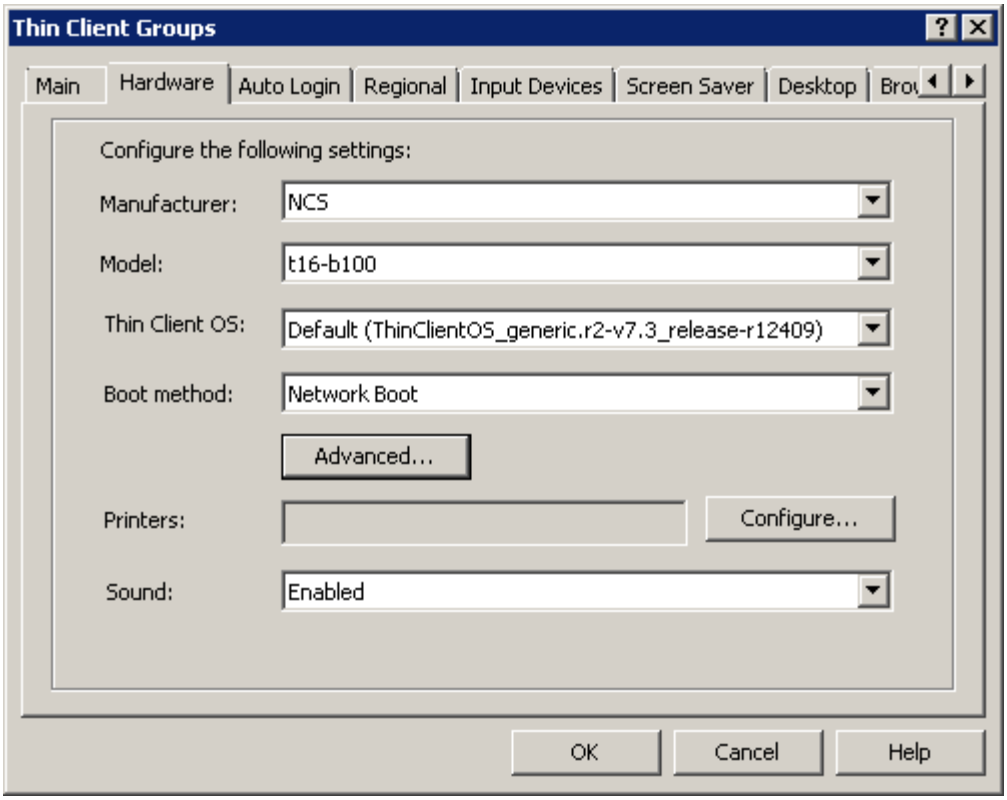
Configuring Hardware Options, OS, Booting Options and Method

In the **Hardware** tab you can configure the following:

- **Manufacturer** and **Model** of the devices in the group from their respective drop down menus. **Note:** By specifying a manufacturer and a model you do not have to configure any boot parameters.
- Version of **Thin Client OS** (2XOS) to use.
- Advanced Configuration and Power Interface (ACPI) settings.
- **Boot method**: specify if the thin clients should make a network boot or install the OS on the thin client hard disk and boot from it.
- **Additional Boot** settings, such as Run OS in debug mode, disable USB devices etc from the **Advanced** button.
- **Printers**: specify which printer should be used. For more information on how to add a printer to the list refer to the section Configuring Thin Client Printers on page 136.
- **Force Display Settings**: click the button **Force Display Settings** to enforce any of the following display settings:
  - Video Card Driver
  - Resolution

- Color Depth
- Refresh Rate
- Support for secondary monitor

- **Sound**: Enable or disable the sound on the thin clients.
- **Enable Terminal Support**: - Like other Linux operating systems, the 2XOS has several terminals. By enabling this option from the **Advanced** button you allow the logged in users to access such terminals and issue operating system commands through them.



Configuring Hardware options for a Thin Client Group

Configuring Auto Login Options

You can enforce all thin clients in the group to use the same username and password and auto login to the 2X ApplicationServer XG from the **Auto Login** tab.

Configuring Regional Settings

Click on the **Regional** tab to configure any of the following regional settings:

- Region
- Country
- Language

Configuring Input Devices

From the **Input Devices** tab you can configure the following settings:

- Mouse model, acceleration and sensitivity
- Keyboard model, layout, repeat rate and delay

Configuring Screen Saver

From the **Screen Saver** tab you can enable or disable the screen saver, screen saver wait time and to automatically lock the desktop.

Configuring Desktop

From the **Desktop** tab you can configure any of the following options (refer to the 2XOS manual for more information about the desktop options):

- Desktop Manager
- Background Colour
- Background Text
- Font Support
- Panel Type
- Windows Manager

Configuring Browser

From the **Browser** tab you can:

- Enable or disable the browser on the 2XOS
- Specify browser type (Opera or Chromium)
- Enable browser in full screen mode
- Configure the browser name, homepage, proxy settings and bookmarks

Configuring Remote Desktop Options

From the **Remote Desktop** tab you can configure remote desktop clients and connection options. It is possible to configure the following remote desktop clients:

- RDP
- VMWare View
- VNC

Note: When the device is configured in kiosk mode, the screen resolution of all the clients is automatically set to full screen.

Configuring Thin Client in Kiosk Mode

In Kiosk mode one application is automatically started in full screen mode once the user logs in. From the **Kiosk** tab you can enable or disable Kiosk mode and specify which applications are automatically launched. The applications that can be launched in kiosk mode are:

- Browser
- RDP
- VMWare View
- VNC

Configuring List of Locally Installed Applications

From the **Local Applications** tab you can specify to enable or disable any of the applications listed below in a managed OS:

- Skype
- Adobe PDF Reader
- Accessories (such as media player, calculator, editor etc)

Configuring Shadowing

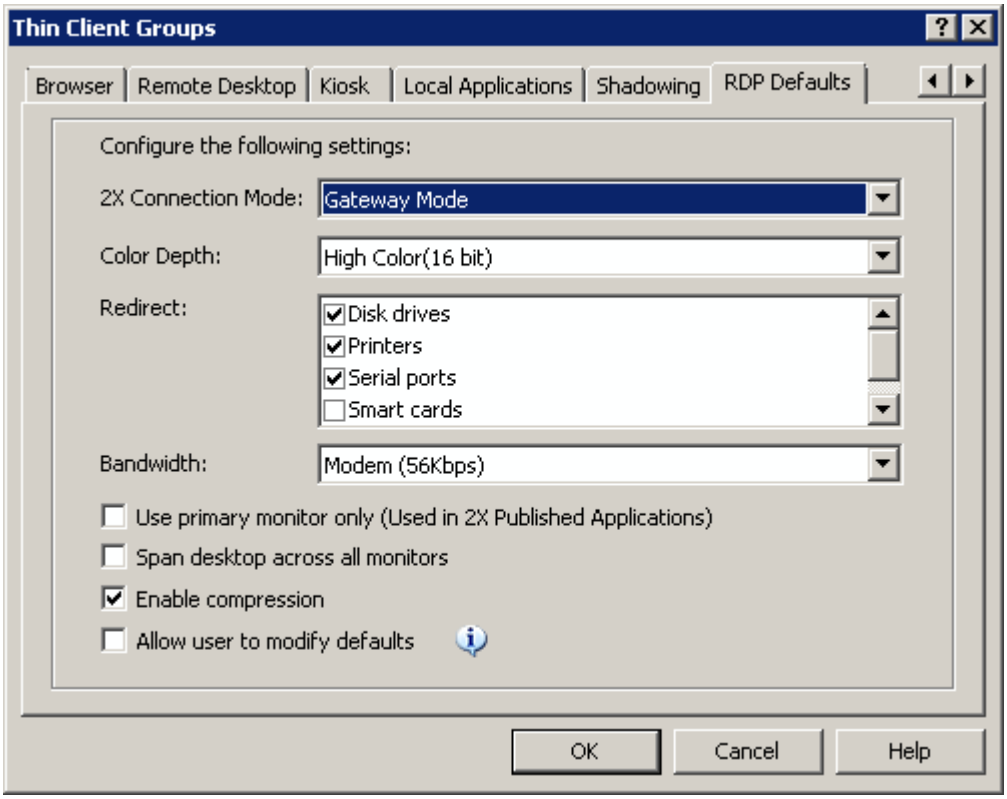
Shadowing allows the administrator to remotely connect with the managed devices, view and interact with the desktop. From the **Shadowing** tab you can:

- Enable and disable shadowing
- Enable and disabled interaction with the desktop
- Password protect the shadowing
- Enable authorization so the user on the client has the option to authorize or not a shadowing session.

Configuring RDP Default settings

From the **RDP Defaults** tab you can configure the settings the thin client uses to connect to the 2X ApplicationServer XG or to the RDP Remote Desktop if enabled. The options available are:

- **2X Connection Mode**: Specify if the user on this device should connect to the 2X ApplicationServer XG using Gateway Mode or Direct Mode using SSL or not.
- **Color Depth**
- **Redirect**: specify which devices on the thin client should be redirected when connected to a session, such as printers, disk drives etc.
- **Bandwidth**
- Multiple monitor options (restrict to one monitor or span desktop across all monitors)
- Disable or **Enabled compression**
- Disallow or **Allow users to modify defaults**



Configuring 2X ApplicationServer XG Connection Settings for a Thin Client Group

Note: The user has the possibility to override these settings if the **Allow user to modify default** option is enabled.

Configuring Thin Client Options

To configure a thin client running the 2XOS, navigate to the **Devices** tab in the **Client Manager** category, highlight the thin client name and click **Properties** from the **Tasks** drop down menu. From the thin client properties you can configure all of the settings mentioned in the section on Configuring Thin Client Options in Groups page 132 of this manual.

If the thin client is part of a group and is already inheriting such options, untick the option **Use Group Settings** from the tab and configure the needed settings to override the group settings.

Configuring Thin Client Printers

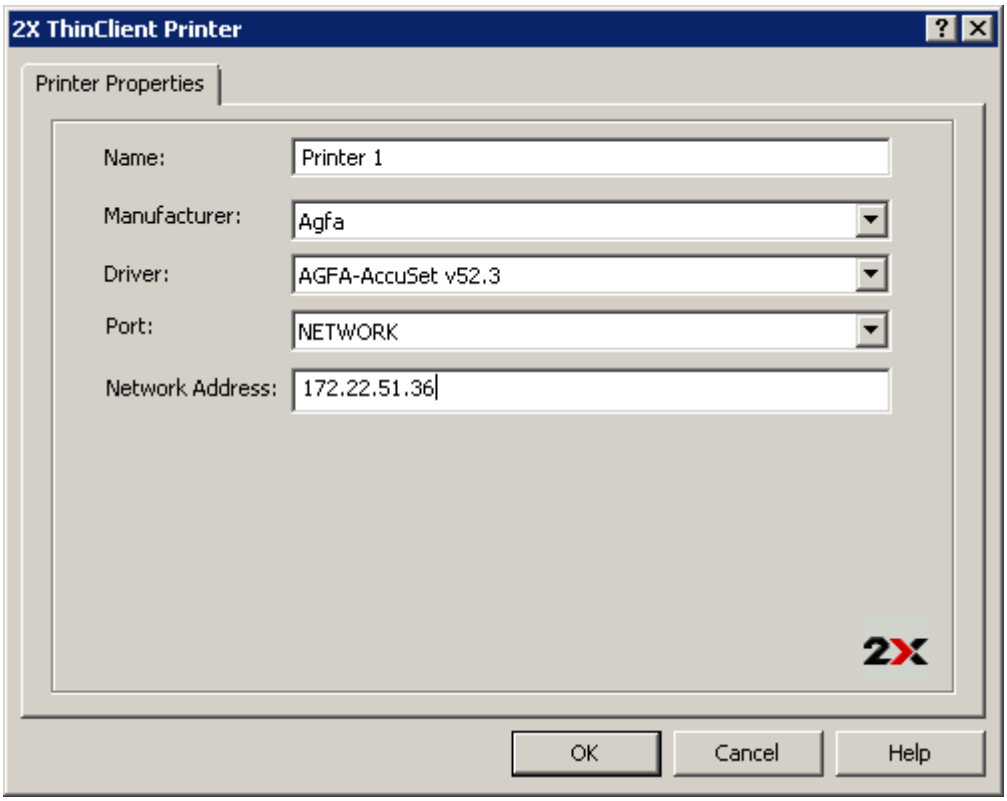
To allow thin clients to use both network printers and local printers connected to them via a parallel or USB port specify the printers in the **List of thin client printers** available from the **Printers** tab in the **Client Manager** category. By specifying printers in this section their drivers are automatically loaded in the 2XOS upon boot up.

Adding a Printer to the List

To add a printer to the **List of thin client printers** click **Add** from the **Tasks** drop down menu and:

- Specify a printer friendly name in the **Name** input field
- Select the printer manufacturer from the **Manufacturer** drop down menu
- Select the printer driver from the **Driver** drop down menu
- Select the connection type from **Port** dropdown menu. If it is a network printer, select **Network** and specify the IP address in the **Network Address** input field.

Click **OK** once the settings are finalized to add the printer to the list.

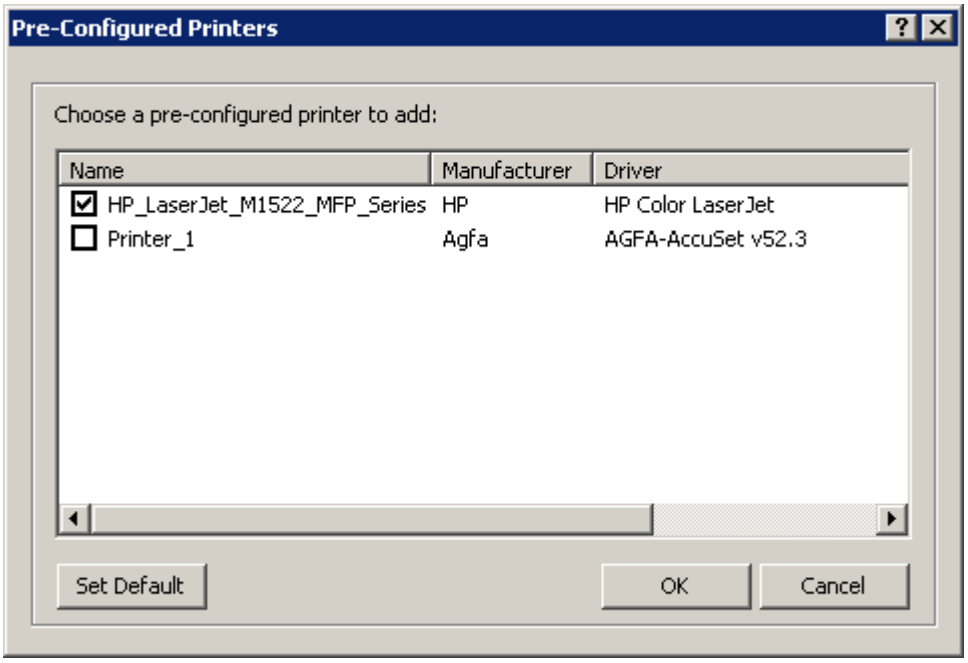


Configuring a Printer for Thin Clients

Assigning a Printer or Multiple Printers to a Thin Client or Group

To assign a printer or multiple printers to a thin client or a group of thin clients follow the below procedure:

1. Access the thin client or group properties
2. Click on the **Hardware** tab
3. Click on **Browse** (**...**) button next to the **Printers** option
4. Select a printer or multiple printers from the list and click **Add**



Adding Printers to a Thin Client or Group

Configuring a Custom 2XOS Log In Banner

You can configure a custom 2XOS log in banner from the **Banner** tab in the **Client Manager** category. Click the option **Custom Banner** and the **Change Custom Banner** button to browse and select the custom banner.

Click back the option **Default Banner** to re-enable the default 2X log in banner.

Scheduling Thin Clients Auto Power On, Off or Restart

Introduction

From the **Scheduler** tab in the **Client Manager** category you can schedule auto powering on or off, and restarting of a thin client or a group of thin clients.

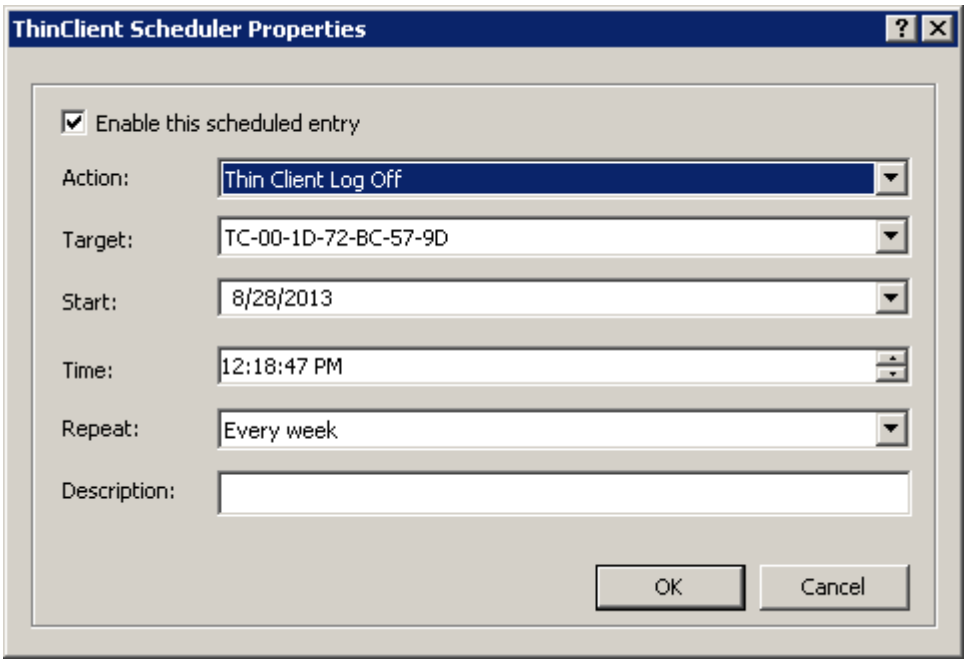
Adding a New Schedule

To add a new schedule follow the below procedure:

1. Click **Add** from the **Tasks** drop down menu and enable the option **Enable this scheduled entry**
2. Select the action from the **Action** drop down menu. Actions available are:
    a. Thin Client Switch On
    b. Thin Client Log Off
    c. Thin Client Switch Off

d. Thin Client Reboot
e. Thin Client Group Switch On
f. Thin Client Group Log Off
g. Thin Client Group Switch Off
h. Thin Client Group Reboot

3. Depending on the action option, select a thin client or a group from the **Target** drop down menu.
4. Specify the start date and time of action from the **Start** and **Time** options.
5. If you would like the schedule to be repeated, specify a frequency from the **Repeat** drop down menu. The options are:
    a. Never
    b. Every day
    c. Every week
    d. Every 2 weeks
    e. Every month
    f. Every year
6. Specify a friendly schedule description name in the **Description** input field and click **Ok** once the schedule is correctly configured.



Scheduling Thin Client or Group Maintenance

Managing Schedules

Modifying an Existing Schedule

To modify an existing schedule highlight the schedule name from the **Schedule List** and click **Properties** from the **Tasks** drop down menu.

Enabling or Disabling a Schedule

To enable a disabled schedule tick the checkbox next to the schedule name or tick the option **Enable this scheduled entry** from the schedule properties. To disable the schedule untick any of the options.

Executing a Schedule

To execute a schedule without waiting for the configured time, highlight the schedule name from the **Schedule List** and click **Execute Now** from the **Tasks** drop down menu.

Deleting a Schedule

To delete a schedule highlight the schedule name and click **Delete** from the **Tasks** drop down menu.

Managing 2X Client Settings

Introduction

From the **2X Client Management** tab in the **Client Manager** category you can manage the 2X Client settings policies for all the users on the network that connect to any server in the Farm. By adding 2X Client Policies you can group users and push different 2X Client settings and options to the users depending on the policy.

Note: These policies only apply to 2X Clients installed on Windows (including Windows CE and XP Embedded). Device Licenses are not needed to use this option.

Adding a New 2X Client Policy

To add a new 2X Client Policy follow the below procedure:

1. Navigate to the **2X Client Management** tab in the **Client Manager** category and click **Add** from the **Tasks** drop down menu.
2. Specify a **Policy Name**.
3. Specify for which Users & Groups the client policy applies to from the **Users & Groups** section by selecting a browse mode from the **Browse Mode** drop down menu and clicking **Add**. **Note**: Preferred browsing mode is Secure Identifier. Other options should only be used for backward compatibility.

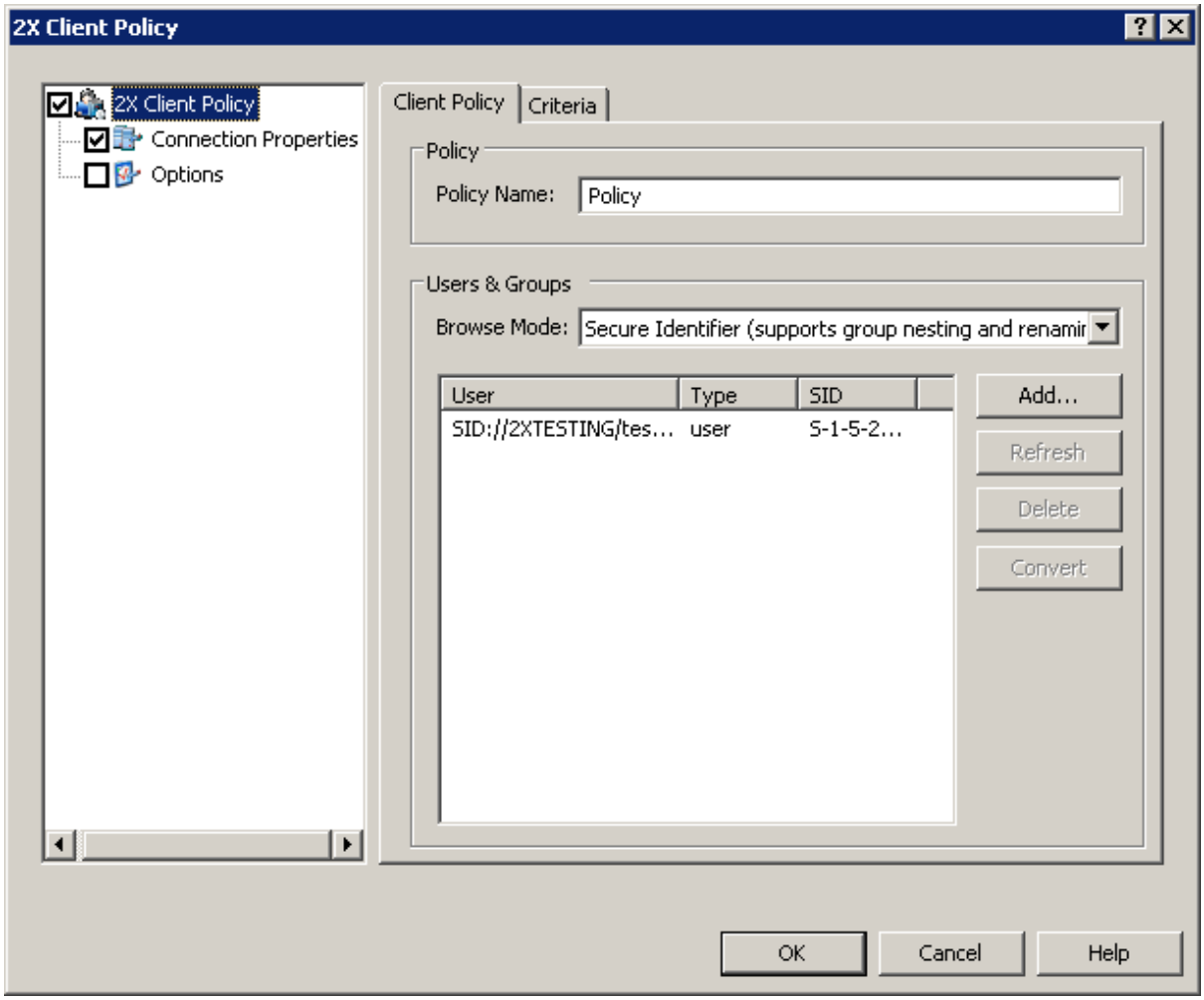
(Optional) Configure Criteria for the Client Policy

By default a client policy applies to the configured users and groups in all situations. You can configure a criteria so the policy only applies when the criteria is matched. Criteria allow you to create different policies for the same user which will be applied depending from where the user is connecting and from which device. To create a new criteria follow the below procedure:

4. Click on the **Criteria** tab.
5. Specify a list of gateways the user is or is not connected to from the **Gateway** section.
6. Specify a list of MAC addresses to match or not the user's MAC address specified in the list from the **MAC Address** section.

Configure Connection Properties and Options

7. Tick the **Connection Properties** node to specify which of the options to restrict or enforce for the 2X Client users.
8. Tick the **Options** node to specify which of the options to restrict or enforce for the 2X Client Users.



Configuring 2X Client Policies to Manage 2X Clients

For more information about the 2X Client, Connection Properties and Options refer to the **2X Client Manual** available online from the 2X documentation page; http://www.2x.com/documentation/.

Reporting

Introduction

To generate 2X ApplicationServer reports a third party provider application called eG Innovations has to be used. eG Innovations is available at an additional cost.

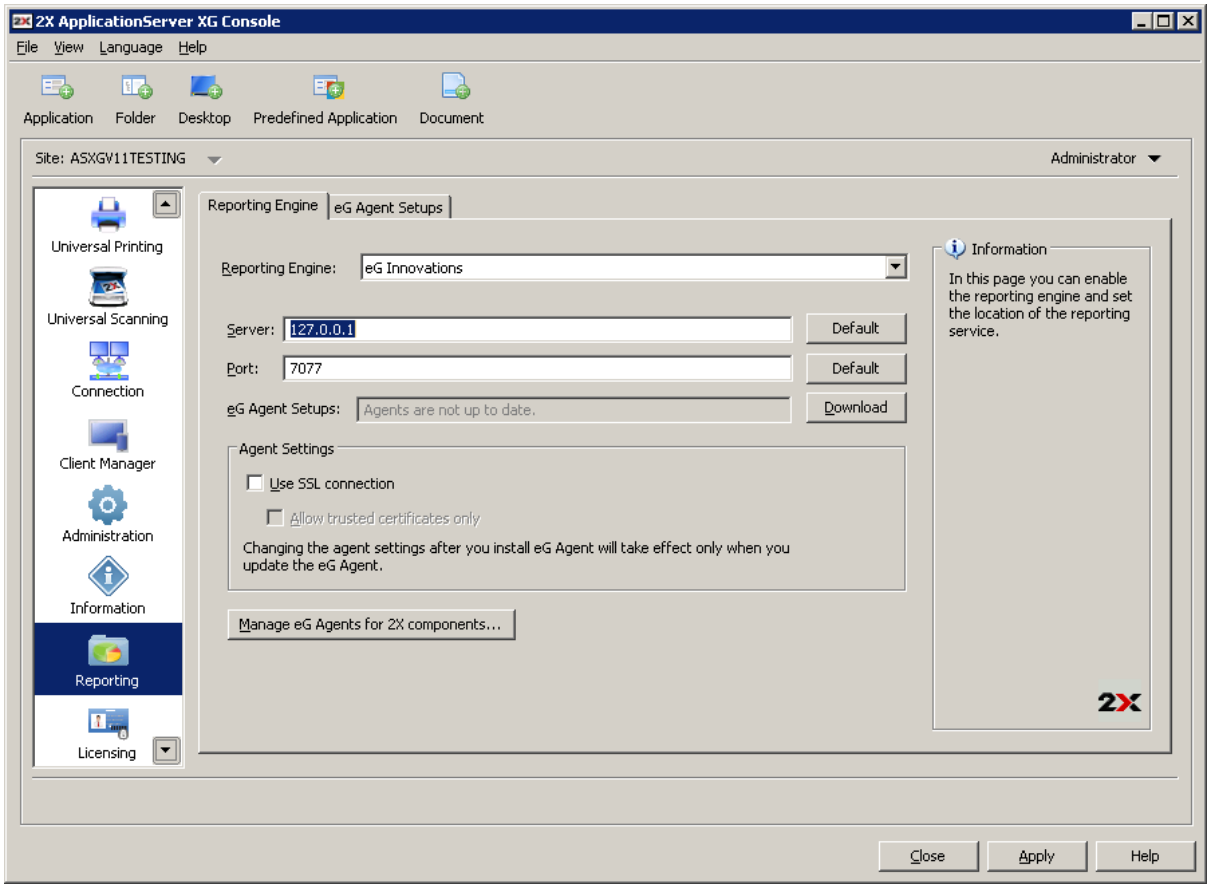
The integration for reporting can be configured from the **Reporting** node in the 2X ApplicationServer Console.

Integrating with eG Innovations Reporting Engine

Configuring the Connection

To integrate 2X ApplicationServer with the eG Innovations reporting engine follow procedure below:

1. Open the 2X ApplicationServer console and click on the **Reporting** node in the navigation bar.
2. Select **eG Innovations** from the **Reporting Engine** drop down menu.
3. Specify the eG Innovations server and port in their respective input fields.
4. (Optional) Enable the option **Use SSL connection** to encrypt the communication between the reporting engine server and the agents.
5. (Optional) Enable the option **Allow trusted certificates only** to enforce the use of trusted certificates only and not accept other types of certificates, such as self-signed certificates.

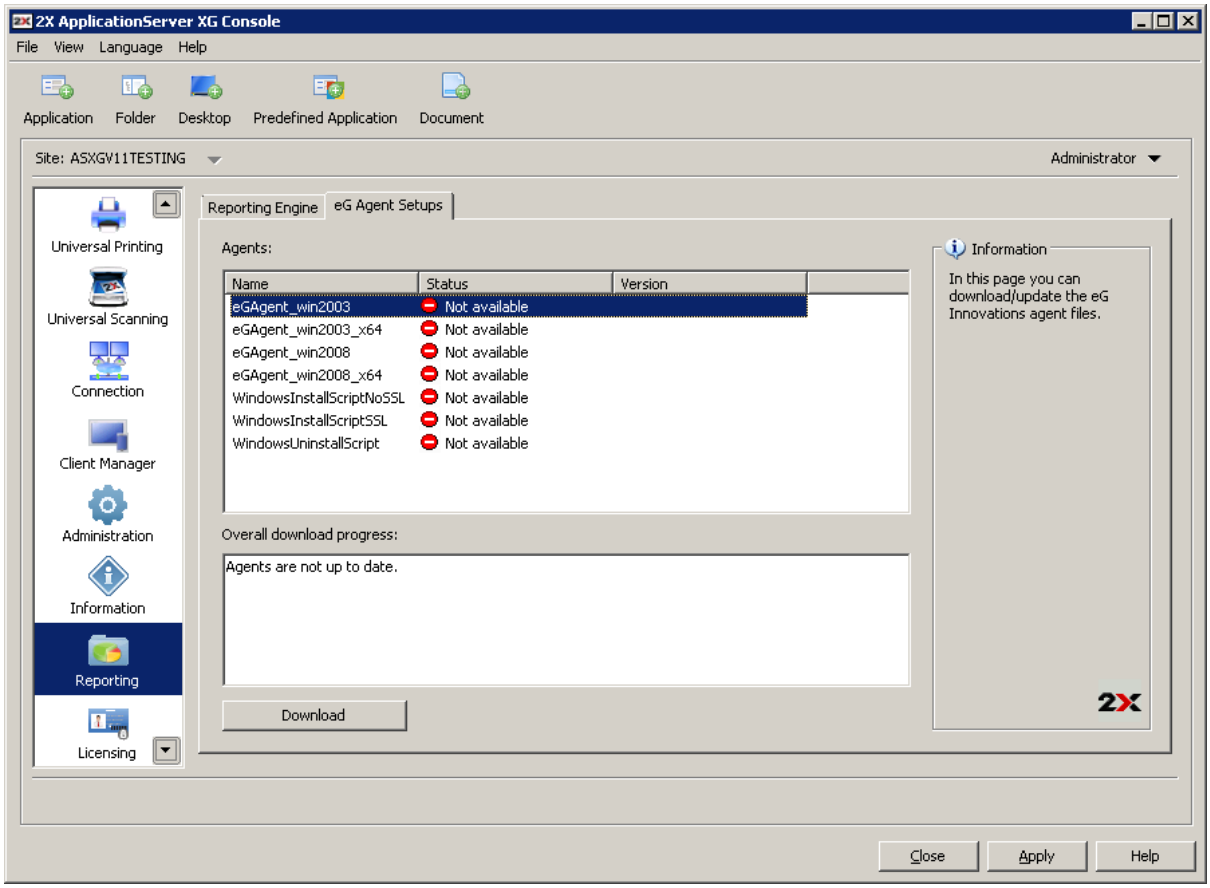


Configuring eG Innovations Integration for 2X Reporting

Configuring the Reporting Agents

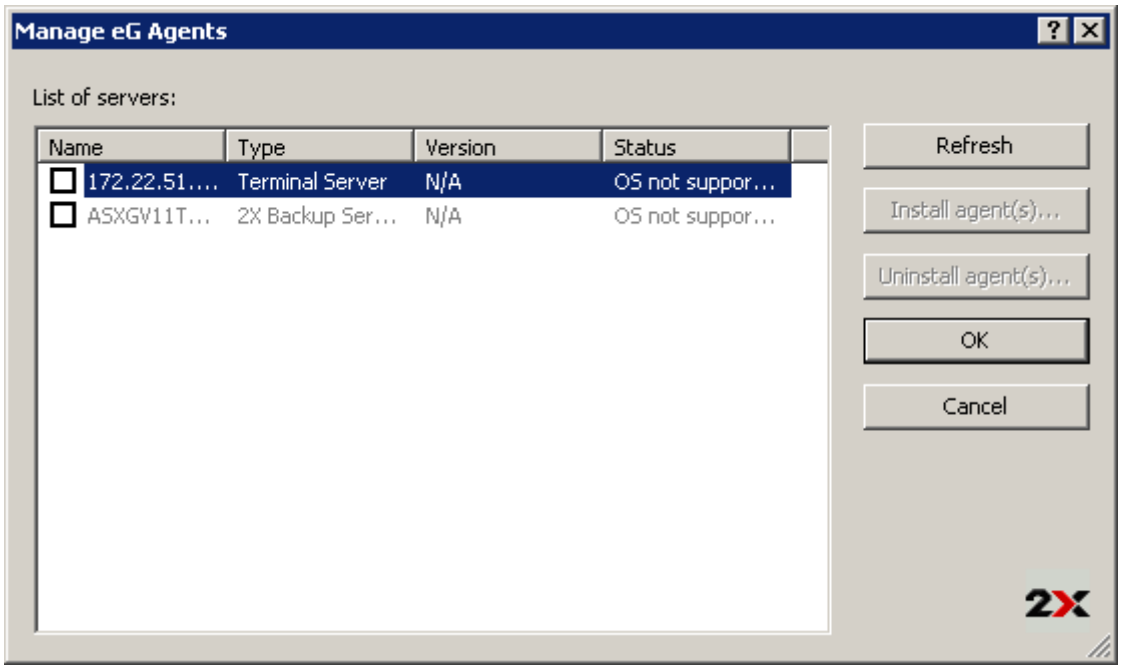
Once the connection between the 2X ApplicationServer and the eG Innovations server is successful, you have to download and install the agents on the servers. To do so, follow the below procedure:

1. Click the **Download** button in the **Reporting Engine** tab to download the latest eG Agents.
2. Once the agents are downloaded you will be automatically switched to the **eG Agent Setups** tab from where you can see the list of agents available.



Download eG Agents from the eG Aget Setups Tab

3. Switch back to the **Reporting Agent** tab and click **Manage eG Agents for 2X components** to start installing the agents on the server.



Managing eG Agents

4. Tick the names of the servers where you want to install the reporting agents and click **Install agent(s)**. **Note:** The reporting agent install process is identical to the 2X Agent install process.

Note: Only servers with 2X Terminal Server agents installed can be managed for eG Agents. Otherwise the servers are not listed.

More Information

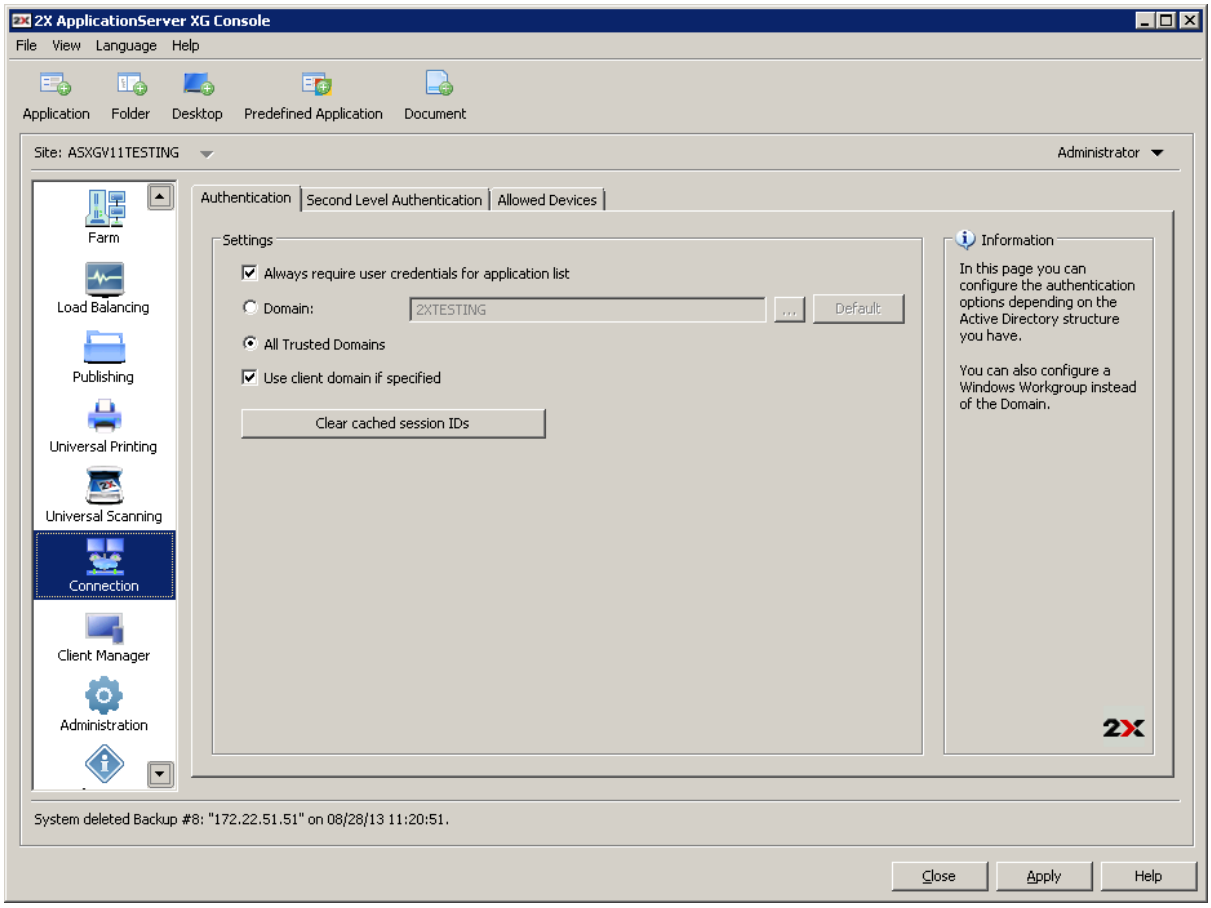
For more information about the 2X ApplicationServer and eG Innovations reporting engine integration refer to the following URL:

http://eginnovations.wordpress.com/2011/12/22/2x-software-selects-eg-innovations-to-provide-monitoring-and-performance-management/

Connection & Authentication Settings

2X Publishing Agent Connection Settings

The 2X Publishing Agent connection settings can be accessed from the **Connection** category available in the system menu.



Configuring Publishing Agent Authentication Settings

Enforcing Authentication

By default all users are required to authenticate the connection against a 2X ApplicationServer XG before accessing any published application or desktop. You can disable such requirement by disabling the option **Always require user credentials for application list** from the **Authentication** tab.

Configuring Authenticating

Once authentication is enforced you can also configure the 2X ApplicationServer XG to authenticate users against a specific domain by entering the domain name in the **Domain**

input field. Alternatively use the **Browse** button to select a domain or workgroup available on the network.

Note: If the option **Use client domain if specified** is disabled the domain name specified by the administrator will be automatically populated in the 2X Client.

Recommendation: After changing the domain names or some other authentication related changes click the **Clear cached session Ids** button.

Authenticating Against Multiple Domains

If the users connecting to the 2X ApplicationServer XG are stored in different domains within a forest, tick the option **All Trusted Domains.**

Authenticating Against Non Domain Users

In order to authenticate users sessions against users specified on a standalone machine you must enter the **[workgroup_name] / [machine_name]** instead of the domain name. For example if you would like to authenticate users against a list of local users on a machine called **SERVER1** that is a member of the workgroup **WORKGROUP**, enter the following in the domain field: **WORKGROUP/SERVER1**.

Second Level Authentication

By configuring a second level of authentication you are providing a higher level of security.

How it Works

Users will have to authenticate through two successive stages to access their network. While the first level of authentication will use the native authentication (Active Directory / LDAP) the second level of authentication can be provided by using one of the following:

- Deepnet Authentication Server
- Safenet Server
- Radius Server

Second level of authentication is more secure because as opposed to first level authentication, instead of using a standard username and password it uses a static username and a onetime password generated by a token.

Second Level Authentication can be configured from the **Second Level Authentication** tab in the **Connection** category.

Configuring Deepnet Authentication Server

For more information on how to configure the Deepnet Authentication Server and 2X ApplicationServer XG integration refer to the **Working with Deepnet** user manual available from the link.

Configuring Safenet Server

For more information on how to configure the Safenet Authentication Server and 2X ApplicationServer XG integration refer to the **Working with Safenet** user manual available from the link.

Configuring Radius Server

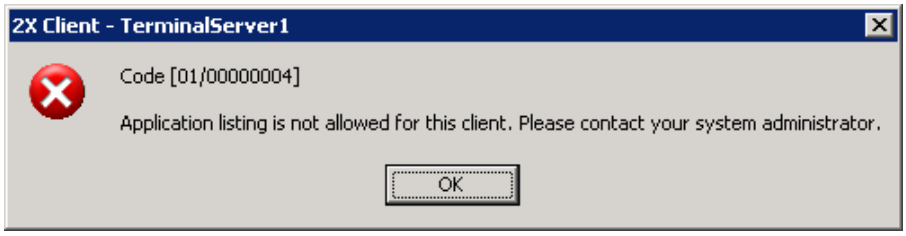
For more information on how to configure the Radius Server and 2X ApplicationServer XG integration refer to the **Working with Radius** user manual available from the link.

Restricting Access by OS Build Number

From the **Allowed Devices** tab you can configure what version the client software should be running to be able to access the system. To restrict such rules, enable the option **Allow connection from these clients only**.

To enable or disable a specific client, tick or untick the tick box next to its name. To modify the build number, highlight the client name in the list and select **Edit** from the **Tasks** drop down menu.

By enabling this option the build number of the client software will be checked and if the build number is lower than the configured one, the client will be receive an error as seen in the screenshot below.


2X Client - TerminalServer1
Code [01/00000004]
Application listing is not allowed for this client. Please contact your system administrator.
OK

Error received by the client when using an older build than the one configured

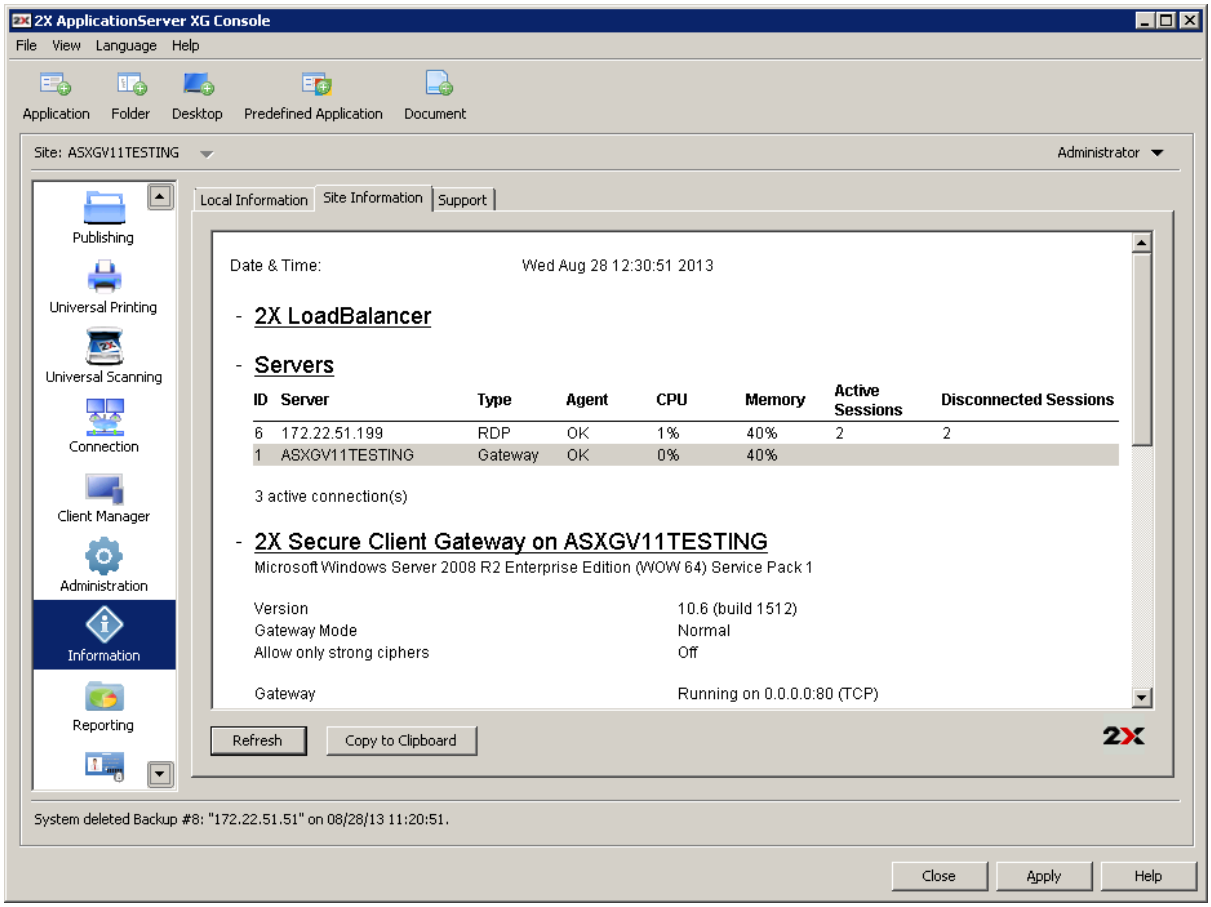
Managing the 2X ApplicationServer XG

Introduction

The 2X ApplicationServer XG also has several features which allow you to monitor the activity on the farm and configure system notifications and several other options.

2X ApplicationServer XG Status

From the **Local Information** tab in the **Information** category you can get an overview of the 2X ApplicationServer XG services running on the server you're logged on. You can also get an overview of the servers on the site you are logged on to, sessions and more from the **Site Information** tab.



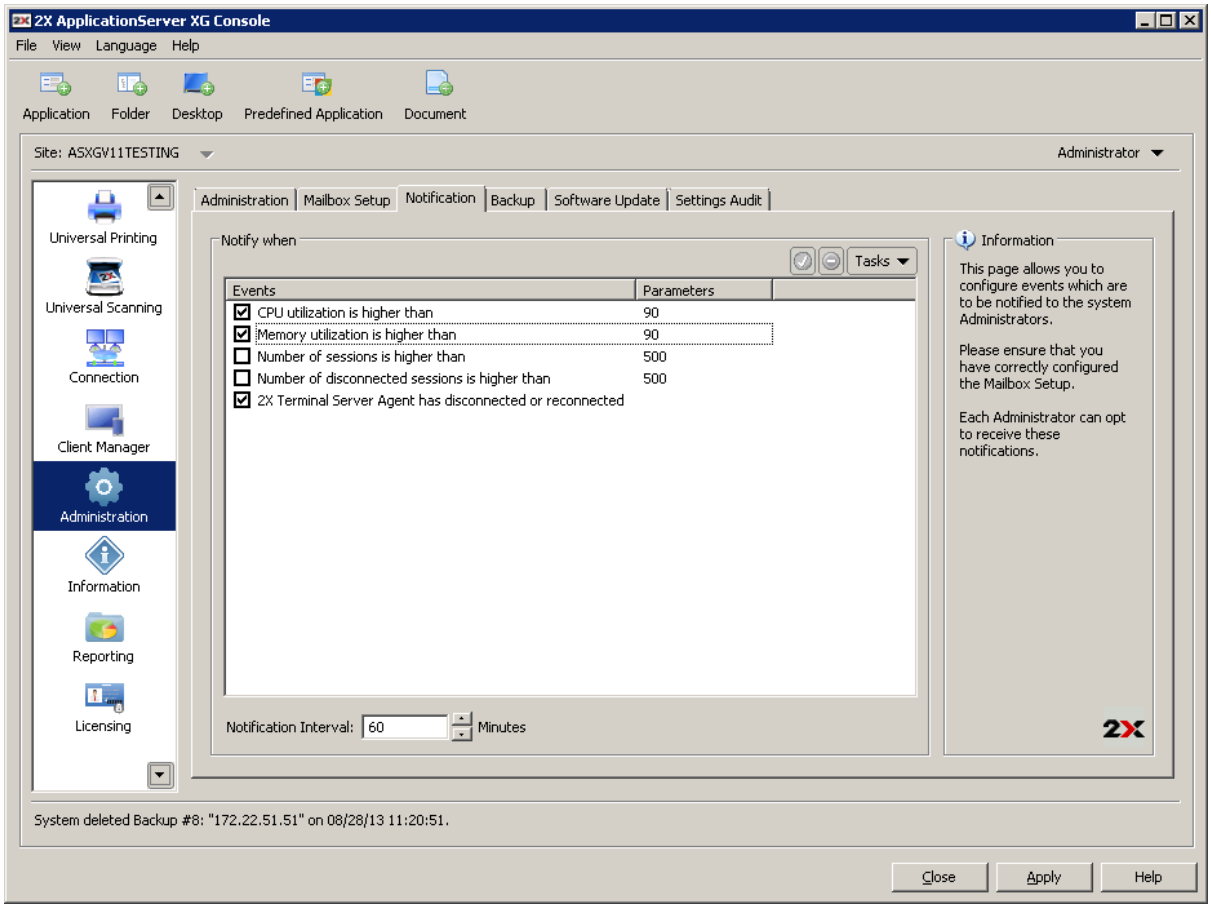
Site Information Tab

Configuring Monitoring Counters and Email Alerts

Configuring Monitoring Counters

From the **Notification** tab in the **Administration** category you can enable, disable and configure different notification counters so once triggered administrators are alerted via email. These settings apply to all servers in the farm. You can configure the following type of monitoring:

- CPU utilization on a server is higher than the configured amount
- Memory utilization on the server is higher than the configured amount
- Number of sessions connected to a server is higher than the configured amount
- Number of disconnected sessions is higher than the configured amount
- 2X Terminal Server Agent has disconnected or reconnected to the farm

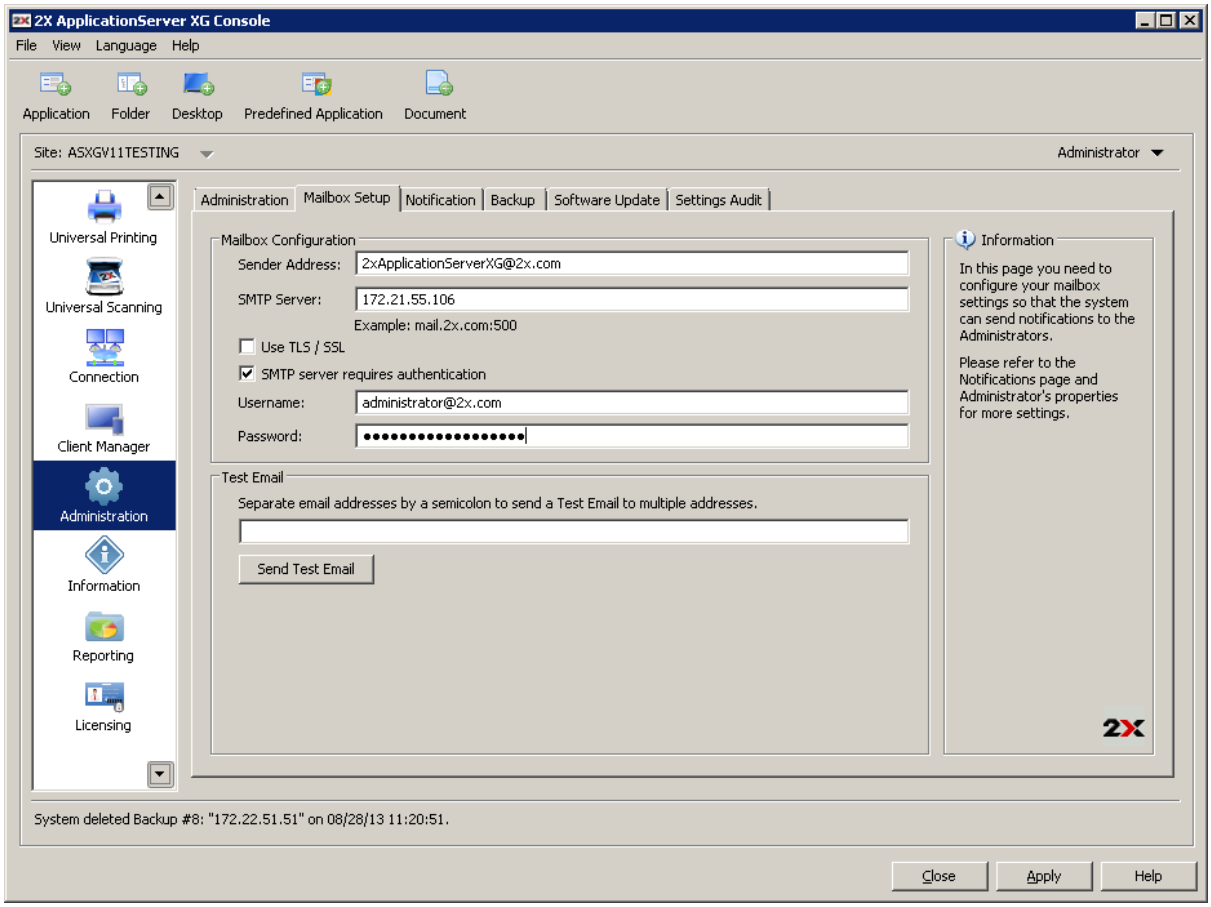


Configuring Monitoring Counters

Configuring SMTP Server Connection for System Notifications via Email

Once monitoring counters have been configured, the SMTP server connection details should be configured from the **Mailbox Setup** tab so the system can send emails once a monitoring counter is triggered. Below is a list of settings that should be configured from the **Mailbox Setup** tab so the server can send emails:

- Sender Email Address
- SMTP Server IP or FQDN
- Disable or enable TLS / SSL encrypted communication
- SMTP Server Credentials in case the SMTP server requires authentication


2X ApplicationServer XG Console
File View Language Help
Application Folder Desktop Predefined Application Document
Site: ASXGV11TESTING
Administrator
Universal Printing
Universal Scanning
Connection
Client Manager
Administration
Information
Reporting
Licensing
Administration Mailbox Setup Notification Backup Software Update Settings Audit
Mailbox Configuration
Sender Address: 2xApplicationServerXG@2x.com
SMTP Server: 172.21.55.106
Example: mail.2x.com:500
Use TLS / SSL
SMTP server requires authentication
Username: administrator@2x.com
Password:
Test Email
Separate email addresses by a semicolon to send a Test Email to multiple addresses.
Send Test Email
Information
In this page you need to configure your mailbox settings so that the system can send notifications to the Administrators.
Please refer to the Notifications page and Administrator's properties for more settings.
System deleted Backup #8: "172.22.51.51" on 08/28/13 11:20:51.
Close Apply Help

Configuring an SMTP Server for Notifications

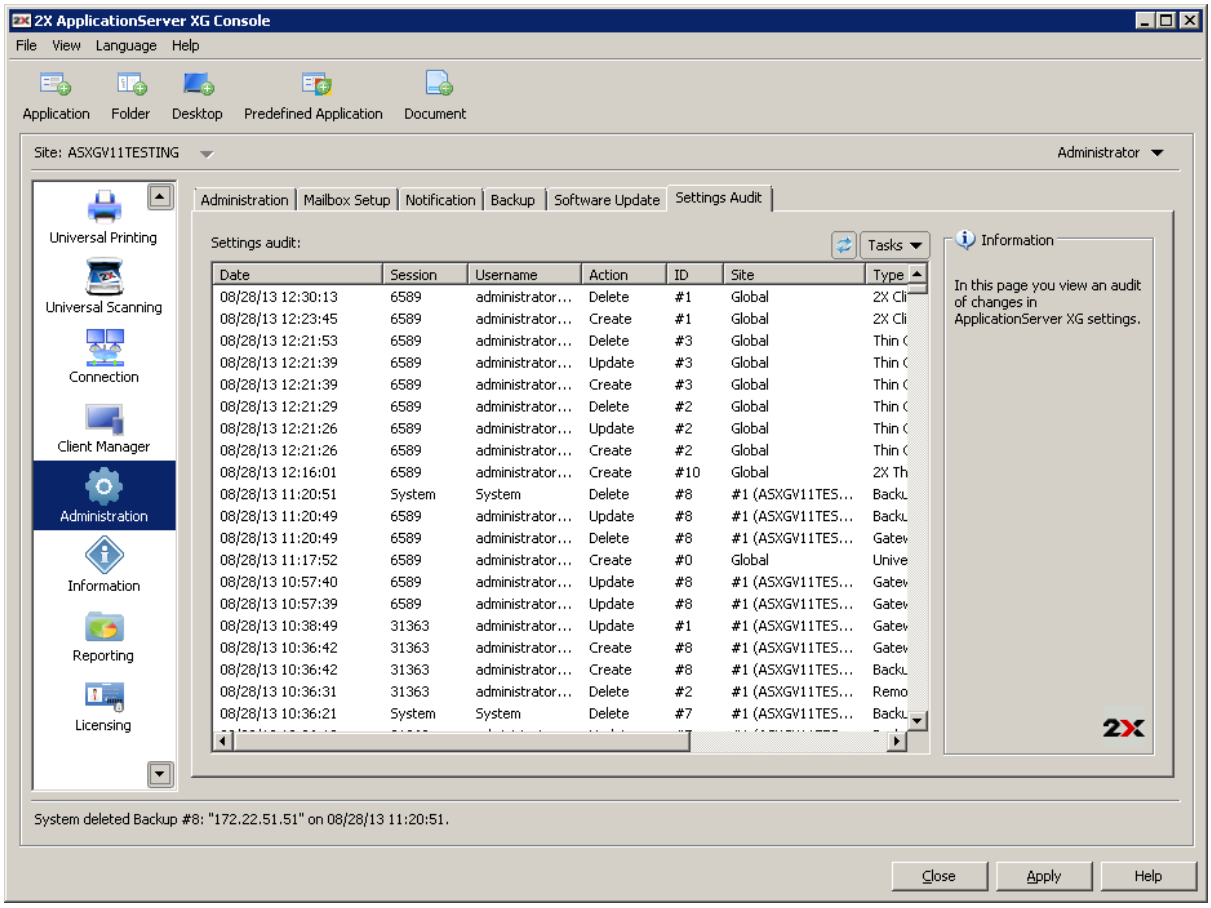
Once the SMTP server connection has been configured, administrator accounts configured to receive system notifications via email will be alerted if a monitoring counter is triggered, for example high CPU usage on a server. To configure an administrator's account notification options, refer to the section Adding an Administrator Account on page 18.

Configuring Notification Intervals

By default a notification is sent every 60 minutes unless the status is changed. You can configure a longer or shorter time frame from the **Notification Interval** option at the bottom of the **Notification** tab.

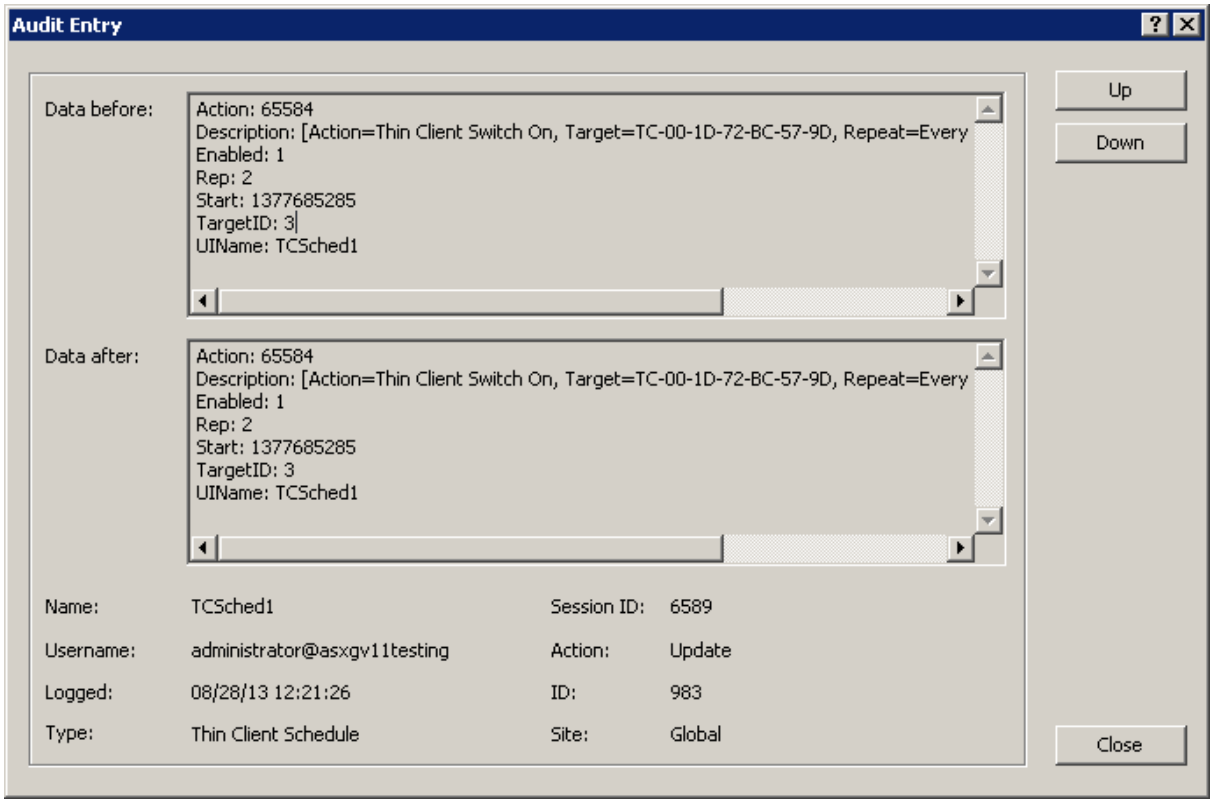
Monitoring 2X ApplicationServer XG Configuration Changes

From the **Settings Audit** tab in the **Administration** category you can see all the 2X ApplicationServer XG configuration changes done by all 2X ApplicationServer XG administrators, as seen in the below screenshot.


2X ApplicationServer XG Console
File View Language Help
Application Folder Desktop Predefined Application Document
Site: ASXGV11TESTING
Administrator
Universal Printing
Universal Scanning
Connection
Client Manager
Administration
Information
Reporting
Licensing
Administration Mailbox Setup Notification Backup Software Update Settings Audit
Settings audit:
Tasks
Information
In this page you view an audit of changes in ApplicationServer XG settings.
Date Session Username Action ID Site Type
08/28/13 12:30:13 6589 administrator... Delete #1 Global 2X Cli
08/28/13 12:23:45 6589 administrator... Create #1 Global 2X Cli
08/28/13 12:21:53 6589 administrator... Delete #3 Global Thin
08/28/13 12:21:39 6589 administrator... Update #3 Global Thin
08/28/13 12:21:39 6589 administrator... Create #3 Global Thin
08/28/13 12:21:29 6589 administrator... Delete #2 Global Thin
08/28/13 12:21:26 6589 administrator... Update #2 Global Thin
08/28/13 12:21:26 6589 administrator... Create #2 Global Thin
08/28/13 12:16:01 6589 administrator... Create #10 Global 2X Th
08/28/13 11:20:51 System System Delete #8 #1 (ASXGV11TES... Backu
08/28/13 11:20:49 6589 administrator... Update #8 #1 (ASXGV11TES... Backu
08/28/13 11:20:49 6589 administrator... Delete #8 #1 (ASXGV11TES... Gatev
08/28/13 11:17:52 6589 administrator... Create #0 Global Unive
08/28/13 10:57:40 6589 administrator... Update #8 #1 (ASXGV11TES... Gatev
08/28/13 10:57:39 6589 administrator... Update #8 #1 (ASXGV11TES... Gatev
08/28/13 10:38:49 31363 administrator... Update #1 #1 (ASXGV11TES... Gatev
08/28/13 10:36:42 31363 administrator... Create #8 #1 (ASXGV11TES... Gatev
08/28/13 10:36:42 31363 administrator... Create #8 #1 (ASXGV11TES... Backu
08/28/13 10:36:31 31363 administrator... Delete #2 #1 (ASXGV11TES... Remo
08/28/13 10:36:21 System System Delete #7 #1 (ASXGV11TES... Backu
System deleted Backup #8: "172.22.51.51" on 08/28/13 11:20:51.
Close Apply Help

Settings Audit Tab where configuration changes are listed

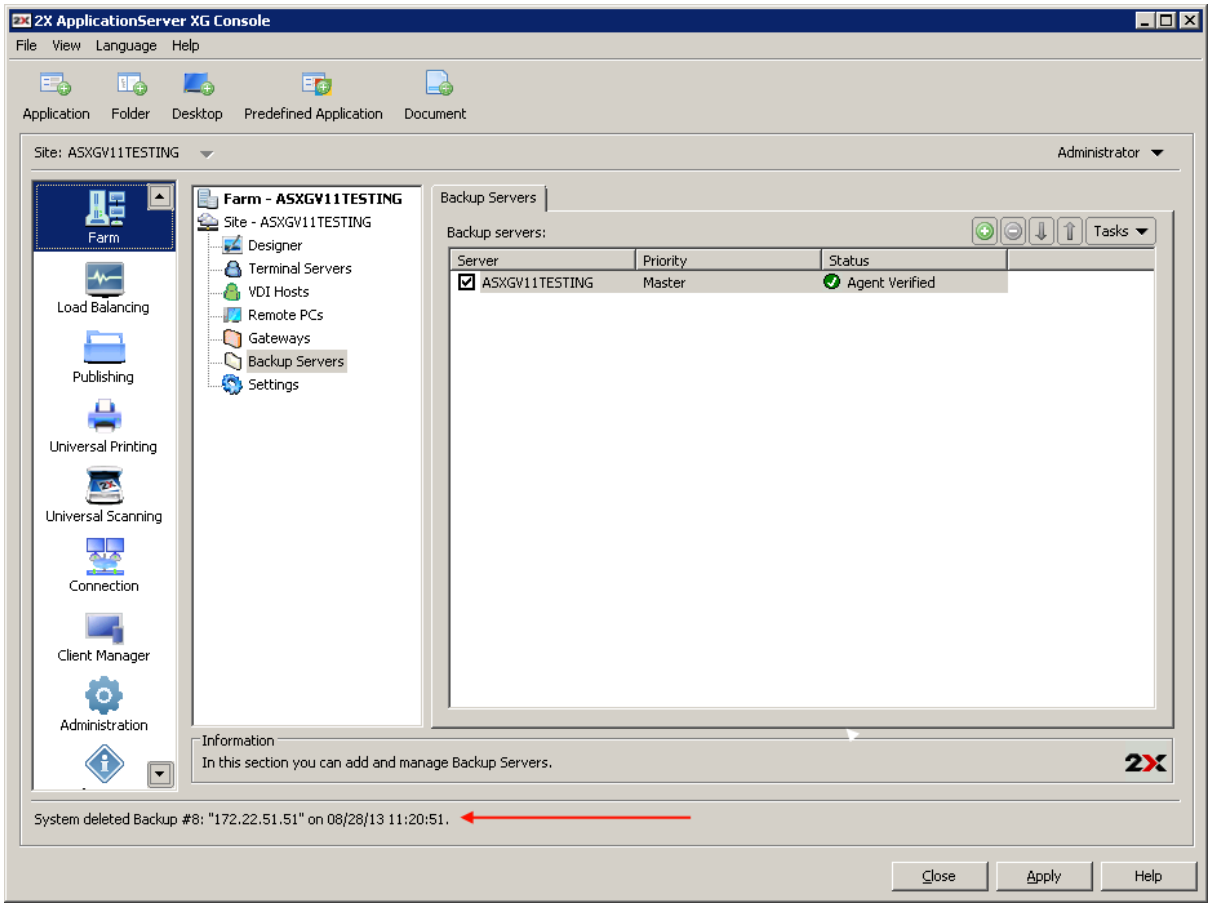
Double click an audit entry to view all the details of the configuration change, as seen in the below screenshot.



Audit Entry details

Configuration Changes Notifications in 2X ApplicationServer XG Console

Each time a logged in administrator applies a configuration change in the farm, a notification message appears at the bottom left corner of the 2X ApplicationServer XG Console so all other logged in administrators are alerted. A configuration change notification is highlighted in the below screenshot.



Configuration Change Notification

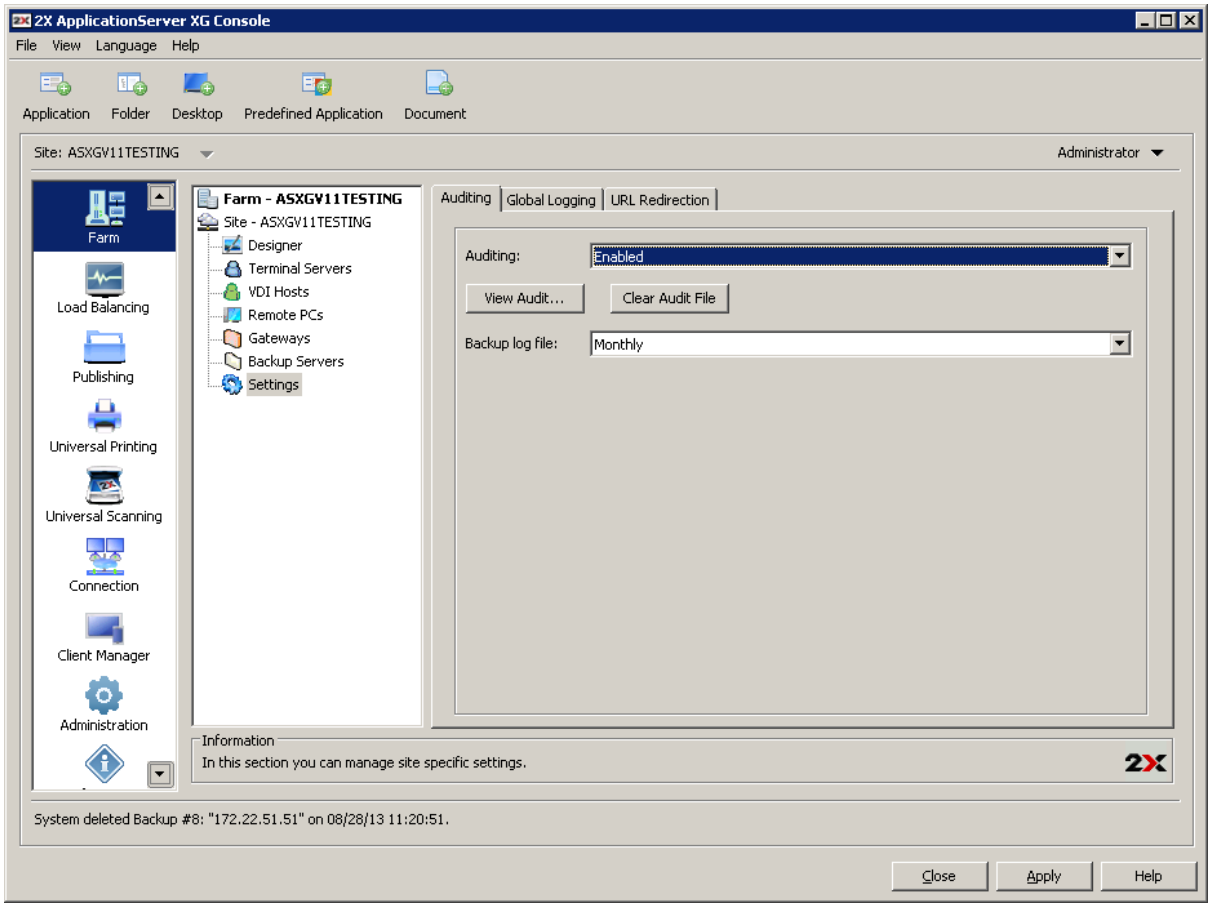
Configuring Logging

By default logging is disabled on the 2X ApplicationServer XG. You can configure per site logging from the **Settings** node of a site in the **Farm** category.

2X ApplicationServer XG Auditing Logging

Introduction

The auditing log contains information about the sessions opened and the total time of each session. Auditing logs can be configured from the **Auditing** tab in the **Settings** node of a site.



Configuring Auditing Logs per Site

Enabling Auditing Logs

To enable auditing logging on a site select **Enabled** from the **Auditing** drop down menu.

Accessing the 2X ApplicationServer Audit Logs

To access the auditing log file click the **View Audit** button from the **Auditing** tab to launch the **2X Monitor**.

Managing 2x ApplicationServer Audit Log Files

To clear the log files click the **Clear Audit File** button. You can also configure log files backup by selecting the backup cycle from the **Backup Log File** drop down menu.

Note: Backup log files are stored in the same directory of the other log files. Backup log files can be viewed from the **Backups** node in the **2X Monitor** application.

2X ApplicationServer XG Logging Per Server

Introduction

The 2X ApplicationServer XG logging is used by the 2X Support Department to troubleshoot an issue therefore it should only be enabled when instructed.

Enabling Logging per Server

To enable logging for a particular server, select the server from the **Farm** category and select **Enable Logging** from the **Tasks** drop down menu.

Viewing Server Logging

To view the log file of a particular server, select the server from the **Farm** category and select **Request Log** from the **Tasks** drop down menu.

Clearing a Server Log File

To clear a server log file, select the server from the **Farm** category and select **Clear Log File** from the **Tasks** drop down menu.

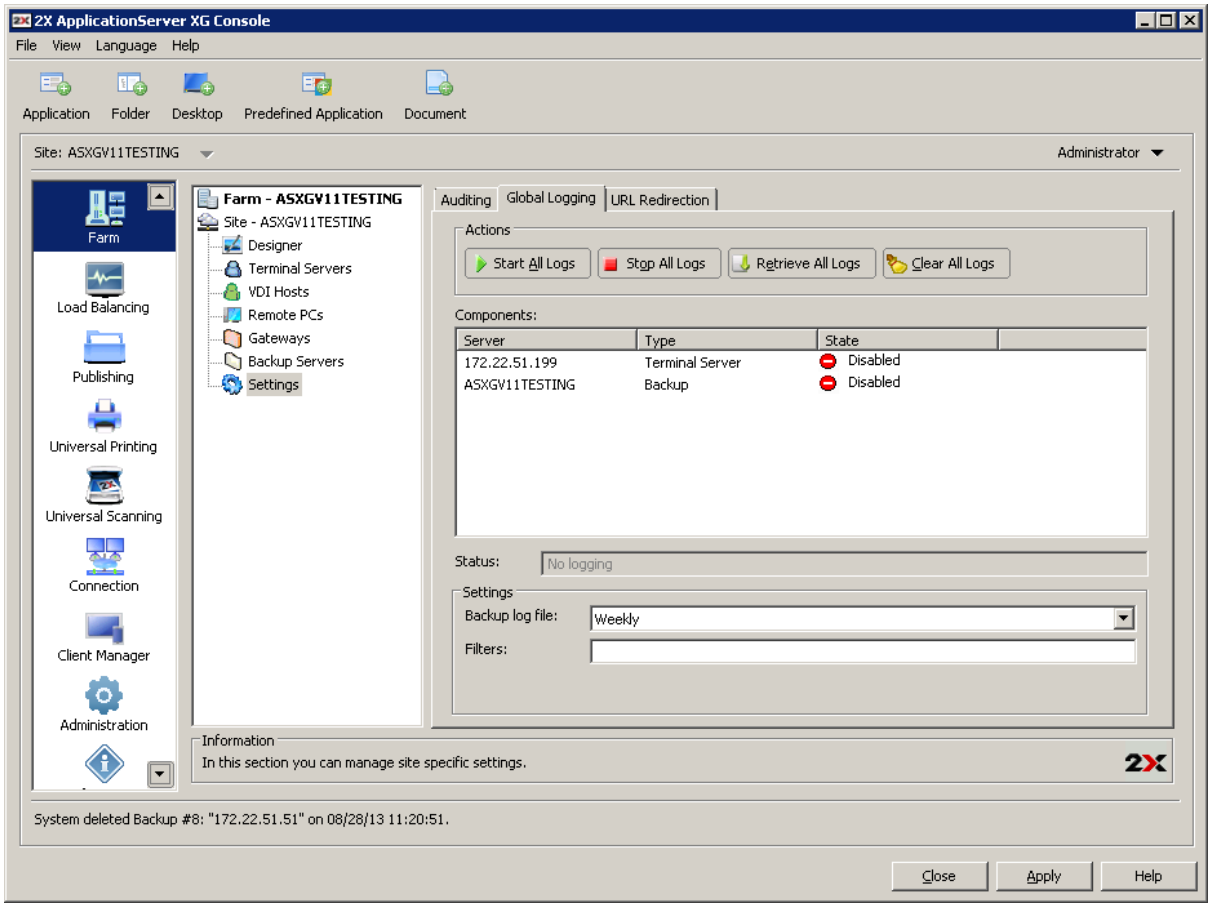
2X ApplicationServer XG Logging Per Site

It is also possible to enable, disable and manage logging globally for all the servers in a site. You can globally manage log files in a site from the **Global Logging** tab in the **Settings** node of a site.

Note: When reporting a problem to the 2X Support it is useful to prepare the log file which can be sent with the support request. To prepare the log file follow the below procedure:

5. Navigate to the **Global Logging** tab
6. Clear all Logs
7. Replicate the problem
8. Stop all logs
9. Retrieve the log files
10. Attach the generated file with the support request

Click the respective button from the **Actions** section to start, stop or clear all logs on each server. Click the **Retrieve All logs** to generate a zip file containing all server log files.



Configuring Server Logging

Keeping 2X ApplicationServer XG Up to Date

By default the 2X ApplicationServer XG will check for updates each time the 2X ApplicationServer Console is launched. You can disable this functionality be disabling the option **Check for updates when launching 2X ApplicationServer XG Console** from the **Software Update** tab in the **Administration** category.

You can also manually check for updates by clicking the **Check Now** button from the **Software Update** tab.

In the same **Software Update** tab a read only list of modules used by the 2X ApplicationServer is available. You do not need to refer to such information unless instructed to do so by the 2X Support Team.

Backing up the 2X ApplicationServer XG Configuration

To backup the 2X ApplicationServer XG farm configuration navigate to the **Administration** category and click **Export** from the **Backup** tab.

Note: A 2X ApplicationServer XG configuration back will only contain the actual configuration. Non related configuration objects such as custom 2XOS banner, downloaded OS etc are not included in the backup.

To restore back a configuration click the **Import** button and navigate to the backup file.

Appendix

2XOS Supported Features

These features are supported by the specified build or higher:

Category	Version	Build
Hardware : Hard Disk Install (Unattended)	7.3	12693
Local Apps	7.3	12188
Multiple Printers	7.3	11878
Printer Ports	7.3	11878
Browser: Chromium	7.3	11596
Boot Parameter: video_rescan	7.2	11370
Boot Parameter: ignore_monitor_edid	7.2	11370
Remote Desktop	7.2	11265
Boot Parameter: delay_kms	7.2	10909
RDP Defaults	7.2	10546
Force Display Settings	7.2	10342

The following features are supported only by the specified Revision:

Category	R1	R2	R3
Browser: Chromium	n/a	n/a	Supported
Desktop: Advanced	n/a	Supported	Supported

The following features are not available in the Compact Version of the 2X Operating System:

Category
Local Apps
Remote Desktop
Desktop: Advanced
Browser

TROUBLESHOOTING AND SUPPORT

Introduction

The troubleshooting chapter explains how you should go about resolving issues you may have. The main sources of information available to users are:

- The manual – most issues can be solved by reading and referring to the manual.
- The 2X support site – accessible from the 2X website. It includes a knowledge base with the most frequently asked questions.
- Contacting the 2X support department by email at support@2x.com
- Contacting our support department by telephone. Contact details available on the 2X Contact Page.

Knowledgebase

2X maintains a knowledgebase, which includes answers to most commonly asked problems. If you have a problem, please consult the knowledgebase first. The knowledgebase is continuously updated and contains the-most-up-to-date listings of support questions and patches.

The knowledgebase can be found at http://www.2x.com/support/

Request Support via E-mail

If you are unable to resolve your issue after using the knowledgebase and referring to this manual, please contact the 2X support department.

Contact us via e-mail, and attach any references or examples of the issue you are experiencing. This will enable us to solve your issue quickly and efficiently.

You may be asked to collect some information and you may be asked a number of questions. Please take your time to answer these questions accurately. Without the proper information it will not be possible to diagnose your problem.

We will answer your inquiry within 24 hours or less, depending on your time zone.

Request Support via Phone

You can also contact 2X by phone for technical support. Please check our support website for the correct numbers to call, depending on where you are located, and for our hours of operation.

ABOUT 2X

2X Software is a global leader in virtual desktop and application delivery, remote access and cloud computing solutions. Thousands of enterprises worldwide trust in the reliability and scalability of 2X products. 2X offers a range of solutions to make every company's shift to cloud computing simple and affordable.

2X Software is a privately held company, with offices in the USA, Germany, UK, Australia, Japan and Malta. 2X holds a Microsoft Gold Competency certification, and partners with IBM, Novell, VMware and many others. Notable 2X customers include Fox News, Harvard University, H&B Foods, McKesson, Advance Auto Parts, Mazda and more.

2X Software's product line includes the award winning 2X ApplicationServer XG providing platform independent virtual desktop, application delivery and integrated thin client management from a single software package; 2XOS for converting desktops PCs into thin clients and the 2X RDP / Remote Desktop Clients for remote access to Windows virtual desktops & applications available for Android, iOS, Chrome OS, BlackBerry and more.

2X Software is the first company to offer integrated thin client management for virtual desktop & application delivery with the 2X ClientManager module for 2X ApplicationServer XG and also the first to provide users with on-demand, proactive protection against both known and unknown attacks through remote desktop connections, ultimately securing access to their home Windows desktop or laptop with 2X SecureRemoteDesktop.